AO

CONSELHO DA JUSTIÇA FEDERAL

PREGÃO ELETRÔNICO Nº 37/2021

PROCESSO SEI: 0004481-11.2020.4.90.8000

DATA: 09 de dezembro de 2021 às 10:00 horas

OBJETO:

"Contratação de solução para gerenciamento de acesso privilegiado (privileged access management - PAM) para proteção dos ambientes computacionais do Conselho da Justiça Federal - CJF, contemplando licenciamento perpétuo, serviços de instalação e configuração, transferência de conhecimento, suporte técnico mensal e garantia para 48 (quarenta e oito) meses".

FORMULÁRIO DE PREÇOS

PROPONENTE: ARVVO Tecnologia, Consultoria e Serviços Ltda;
CNPJ: 25.359.140/0001-81 INSC. ESTADUAL: 07.778.347/001-93
END.: SHN Quadra 1 Bloco A Sala 1.114 – Bairro: Asa Norte – Brasília/DF - CEP: 70.701-010 - FONE/FAX: (61)3553-9006 - SITIO: www.arvvo.com.br E-mail: andre.oliveira@arvvo.com.br
Banco: Itaú Conta Corrente: 97.466-4 Agência: 3213

Senhor Pregoeiro,

Proposta que faz a empresa Arvvo Tecnologia, Consultoria e Serviços Ltda, inscrita no CNPJ n.º 25.359.140/0001-81 e inscrição estadual n.º 07.778.347/001-93, estabelecida no SHN Quadra 1 Bloco A Sala 1.114, CEP: 70.701-010, Brasília-DF, para a contratação supramencionada, de acordo com todas as especificações e condições do Edital e seus Anexos.

Item	Especificação	Fabricante	Qtde	Preço Unitário (R$)	Preço Total (R$)
1.1	Solução para Gerenciamento de Acesso Privilegiado com licenciamento perpétuo de *software* e fornecimento de equipamento(s)	MT4 SENHASEGURA	1	R$ 757.000,00	R$ 757.000,00
1.2	Serviços de instalação e configuração.		1	R$ 9.000,00	R$ 9.000,00
1.3	Serviço de suporte técnico mensal		48	R$ 2.562,50	R$ 123.000,00
1.4	Transferência de conhecimento		6	R$ 1.835,00	R$ 11.010,00
VALOR TOTAL					**R$ 900.010,00**

1) Fornecer preço à vista com tributos, insumos e demais encargos da contratação.

2) Pagamento exclusivamente por ordem bancária.

Obs.: Por força do art. 2º, §3º do Decreto n. 6.306/2007, o IOF não poderá ser incluído no valor da proposta.

VALIDADE DA PROPOSTA: 90 (noventa) dias, contados da data de abertura da licitação.

RAZÃO SOCIAL: ARVVO Tecnologia, Consultoria e Serviços Ltda;
CNPJ (MF) nº: 25.359.140/0001-81;
INSCRIÇÃO ESTADUAL nº: 07.778.347/001-93;
ENDEREÇO: SHN Quadra 1 Bloco A Sala 1.114;
TELEFONE/FAX: (61) 3553-9006
E-MAIL: andre.oliveira@arvvo.com.br;
CEP: 70.701-010;
CIDADE: Brasília ESTADO: Distrito Federal;
DADOS BANCÁRIOS: Banco: Itaú Conta Corrente: 97.466-4 Agência: 3213;

NOME DO REPRESENTANTE LEGAL: André Luiz Alves de Oliveira;
CPF: 705.590.401-30
RG: 1.685.233 - SSP/DF;
E-MAIL: andre.oliveira@arvvo.com.br;

DECLARAMOS, por fim, conhecer e aceitar todas as condições estabelecidas no Edital e seus anexos, bem como nos esclarecimentos publicados pelo **CONSELHO DA JUSTIÇA FEDERAL**, para o referido Edital.

Brasília-DF, 09 de dezembro de 2021

Atenciosamente,

ANDRE LUIZ ALVES DE OLIVEIRA:70559040130

Assinado de forma digital por ANDRE LUIZ ALVES DE OLIVEIRA:70559040130
Dados: 2021.12.09 11:11:44 -03'00'

ARVVO TECNOLOGIA, CONSULTORIA E SERVIÇOS LTDA
André Luiz Alves de Oliveira
Sócio-Diretor

ITEM	Atende	Documentação (Documento, Sessão e Página)
1. Módulo - Cofre de Senhas	**S**	**N/A**
1.1. A solução de cofre de senhas deve ser licenciada de forma a atender os quantitativos mínimos descritos a seguir:	N/A	N/A
1.1.1. Quantidade de servidores Linux: 600;	SIM	Carta Comercial
1.1.2. Quantidade de servidores Microsoft Windows: 150;	SIM	Carta Comercial
1.1.3. Quantidade de estações de trabalho Microsoft Windows: 550;	SIM	Carta Comercial
1.1.4. Quantidade de estações de trabalho Linux: 30;	SIM	Carta Comercial
1.1.5. Quantidade de ativos de rede (switches, roteadores, firewalls, controladores, balanceadores, WAF e outros): 40;	SIM	Carta Comercial
1.1.6. Quantidade de instâncias de bancos de dados: 25;	SIM	Carta Comercial
1.1.7. Quantidade de licenças para cofre de senhas: 40 usuários ou 1395 dispositivos;	SIM	Carta Comercial
1.1.8. Quantidade de aplicações com senha de banco de dados armazenada localmente: 15.	SIM	Carta Comercial
1.2. A solução deve suportar a implementação no parque computacional do CONTRATANTE relacionado no ANEXO II - RESUMO DO AMBIENTE DE TI.	SIM	Carta Comercial
1.3. A solução deve ser implantada localmente nas instalações do CONTRATANTE, com modelo de alta disponibilidade, continuidade de negócios e formas de recuperação de desastre.	SIM	Especificação Técnica - Disponibilidade e Contingência (pag. 28)
1.4. A solução deve prover alta disponibilidade para as funcionalidades deste módulo com opção ativo/passivo ou ativo/ativo, com failover automático para todas as arquiteturas de implantação, com todas as licenças válidas e com garantia igual ao do objeto desta contratação e sem custos adicionais para o CONTRATANTE.	SIM	Especificação Técnica - Disponibilidade e Contingência (pag. 28)
1.5. A solução deve contemplar a expansão, incremento ou melhoria dos métodos utilizados para alta disponibilidade sem qualquer custo adicional de licenciamento da solução para o CONTRATANTE.	SIM	Carta Comercial
1.6. Todos os controles de alta disponibilidade da solução devem ser feitos via interface gráfica, sem depender de comandos manuais, scripts ou adaptações.	SIM	Interface Web Orbit - Chaveamento automático de instâncias (pag. 56)
1.7. A solução deve realizar gerência da sincronização de dados dos servidores/appliances da solução de forma nativa pela solução sem necessidade de intervenção manual.	SIM	Interface Web Orbit - Chaveamento automático de instâncias (pag. 56)
1.8. A solução deve possuir a capacidade de operação de todas as funcionalidades a partir de nós (servidores) físicos e virtuais, permitindo arranjos do tipo: físico-físico ou físico-virtual, sendo que um dos nós ofertados pela CONTRATADA para a solução deve ser físico, obrigatoriamente.	SIM	Especificação Técnica - Disponibilidade e Contingência (pag. 28)
1.9. A solução deve auxiliar no atendimento da Lei Geral de Proteção de Dados (LGPD) no que se refere a:	N/A	N/A
1.9.1. Determinação de como os dados deverão ser tratados, mantidos e protegidos e a quem responsabilizar em caso de descumprimento;	SIM	Auditoria e Rastreabilidade - Rastreabilidade (pag. 15) Especificação Técnica - Políticas de Acesso às informações, senhas e sessões (pag. 10) Especificação Técnica - Compatibilidade ISO 27001, PCI, SOX, GDPR, LGPD, PQO BM&F (pag. 7) Gestão de Usuários - Esquecer um usuário (pag. 14)
1.9.2. Proteção do acesso a dados pessoais;	SIM	Auditoria e Rastreabilidade - Rastreabilidade (pag. 15) Especificação Técnica - Políticas de Acesso às informações, senhas e sessões (pag. 10) Especificação Técnica - Compatibilidade ISO 27001, PCI, SOX, GDPR, LGPD, PQO BM&F (pag. 7) Gestão de Usuários - Esquecer um usuário (pag. 14)
1.9.3. Responsabilização pessoal e resposta a incidentes;	SIM	Auditoria e Rastreabilidade - Rastreabilidade (pag. 15)
1.9.4. Aplicação de boas práticas de governança, através de regras que deverão respeitar os preceitos da lei, de maneira a mitigar os riscos inerentes ao tratamento de dados e implementar e demonstrar a efetividade das políticas de segurança relacionadas ao tratamento de dados.	SIM	Auditoria e Rastreabilidade - Rastreabilidade (pag. 15) Especificação Técnica - Políticas de Acesso às informações, senhas e sessões (pag. 10) Especificação Técnica - Compatibilidade ISO 27001, PCI, SOX, GDPR, LGPD, PQO BM&F (pag. 7)

1.10. A solução deverá operar de forma integrada, ou seja, os softwares, equipamentos e demais componentes fornecidos, bem como as configurações aplicadas pela CONTRATADA, deverão operar como um conjunto plenamente ajustado, de forma a garantir gerenciamento integrado, desempenho, disponibilidade e funcionalidades adequados aos requisitos do CONTRATANTE.	SIM	Especificação Técnica - Módulos do sistema. Arquitetura (pag. 4)
1.11. A solução deve prover mecanismos de atualização de segurança de forma automática e sob demanda por meio de interface gráfica intuitiva.	SIM	Interface Web Orbit - Realizando atualização do sistema (pag. 18)
1.12. A solução deve disponibilizar console de configuração unificada para gerenciamento de contas e ativos agregados ao cofre de senhas.	SIM	Informações Privilegiadas - Introdução (pag. 5)
1.13. A solução não deve depender da instalação de agentes para realizar a troca de senhas ou a gravação de sessão.	SIM	Especificação Técnica - Módulo de troca de senhas (pag. 12)
1.14. A solução deve ser capaz de descobrir credenciais privilegiadas utilizadas por serviços e processos automatizados.	SIM	Scan & Discovery - Credenciais associadas a serviços (pag. 50)
1.15. A solução deve propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas.	SIM	Informações Privilegiadas - Configuração de execução (pag. 13)
1.16. A solução deve ter a capacidade de gerenciar credenciais de sistemas localizados em múltiplas localidades geográficas ou domínios distintos.	SIM	Informações Privilegiadas - Algumas entidades importantes (pag. 6)
1.17. A solução deve possuir interface única para gerenciamento de senhas e sessões, implementada em HTM5 ou cliente único compatível com sistema operacional Microsoft Windows 10 e superiores.	SIM	Especificação Técnica - Compatibilidade com Browser (pag. 30)
1.18. A solução deve possibilitar a integração com ferramentas de Service Desk e de Gestão Mudança com possibilidade de validação de critérios pré-definidos para liberação de acesso.	SIM	Gestão de Usuários - Integração ITSM (pag. 37)
1.19. A solução deve gerenciar de forma segura senhas utilizadas por contas de serviço, evitando a utilização de senhas em texto claro por scripts ou rotinas dos equipamentos.	SIM	App2App - Integração via Webservice (pag. 5)
1.20. A solução deve garantir a aplicação exclusiva de privilégios adequados, provendo acesso às senhas das contas privilegiadas somente ao pessoal autorizado.	SIM	Informações Privilegiadas - Grupos de Acesso para Credenciais (pag. 18)
1.21. A solução não deve limitar o quantitativo de contas que podem ser gerenciadas em um dispositivo licenciado.	SIM	Especificação Técnica - Limite de recurso (pag. 34)
1.22. A solução, em um dispositivo licenciado, deve contemplar sua expansão, incremento ou melhoria sem qualquer custo adicional de licenciamento da solução para o CONTRATANTE.	SIM	Carta Comercial
1.23. A solução deve permitir a opção de implementar o gerenciamento de troca de senhas em redes separadas e dispositivos remotos.	SIM	Especificação Técnica - Módulo de troca de senhas (pag. 12)
1.24. Deve incorporar medidas de segurança, incluindo criptografia a fim de proteger a informação em trânsito entre os módulos distribuídos e entre as aplicações WEB dos usuários finais.	SIM	Especificação Técnica - Criptografia e Recursos de Segurança (pag. 24)
1.25. Deve permitir, através de interface gráfica, administração e configuração de integrações com dispositivos e/ou plataformas que não são disponibilizadas nativamente, sem a necessidade de serviços profissionais de terceiros.	SIM	Informações Privilegiadas - Registrando o Dispositivo (pag. 7)
1.26. A solução deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando scripts, linguagens de programação diversas e aceite protocolos variados incluindo, no mínimo, SSH e HTTP/HTTPS.	SIM	Operações Automatizadas - Sintaxes de plugins executores (pag. 53)
1.27. A solução deve ser disponibilizada com um SDK (Software Development Kit) ou API (Application Programming Interface) que pode ser configurado para permitir que aplicações possam:	N/A	N/A
1.27.1. Solicitar credenciais sob demanda ao invés de utilizar credenciais estáticas;	SIM	App2App - Credenciais (pag. 20)
1.27.2. Atualizar informações de contas automaticamente no banco de dados de senhas;	SIM	App2App - Credenciais (pag. 20)
1.27.3. Inscrever automaticamente em sistemas alvo sem aguardar por atualizações dinâmicas;	SIM	App2App - Credenciais (pag. 20)
1.28. A solução deve proteger as senhas de credenciais compartilhadas que seriam normalmente armazenadas em planilhas e arquivos em texto claro.	SIM	Informações Privilegiadas - Registro de Dispositivos e Credenciais (pag. 6)
1.29. Deve oferecer em sua aplicação diferentes visões e opções de acordo com as permissões dos usuários, mostrando, por exemplo, apenas as funcionalidades delegadas àquele usuário.	SIM	Gestão de Usuários - Camada de Controle de Acesso (pag. 7)
1.30. A solução deve permitir a configuração e emissão de alertas disparados automaticamente pelo sistema, por e-mail e SNMP, para eventos customizados pelo administrador do sistema e que contemplem, no mínimo, os dos seguintes casos:	N/A	N/A
1.30.1. Parada de serviços essenciais;	SIM	Monitoramento e Notificações - Monitoramento (pag. 4)
1.30.2. Alcance do limite de processamento da CPU;	SIM	Monitoramento e Notificações - Monitoramento (pag. 4)
1.30.3. Alcance do limite de processamento da memória;	SIM	Monitoramento e Notificações - Monitoramento (pag. 4)

1.30.4. Alcance do limite de capacidade do armazenamento de dados;	SIM	Monitoramento e Notificações - Monitoramento (pag. 4)
1.31. Caso a solução seja estruturada em componentes, nenhum deles deve conter senhas em texto claro para autenticação.	SIM	Especificação Técnica - Criptografia e Recursos de Segurança (pag. 24)
1.32. Deve permitir a formação de Grupos de Usuários e Dispositivos, bem como a atribuição de Privilégios de Acesso a esses Grupos, onde esses Privilégios de Acessos possam ser atribuídos por critérios como tipo de dispositivo, marca, modelo, fabricante, localidade ou grupo abertos definidos a critério do administrador na própria ferramenta.	SIM	Informações Privilegiadas - Entidades segregadas e suas propriedades (pag. 19)
1.33. A solução deve garantir que a senha gerada tenha a grafia diferente do nome da conta correspondente.	SIM	Carta Comercial
1.34. Permitir a determinação de quais símbolos estão excluídos ou exclusivamente permitidos na composição da senha.	SIM	Informações Privilegiadas - Políticas de credenciais e força de senhas (pag. 66)
1.35. A solução deve permitir que a senha seja segmentada em partes proporcionais ao número de segmentos definidos na política de segmentação da senha, seja por fracionamento da senha, seja mediante autorização por múltiplos aprovadores.	SIM	Informações Privilegiadas - Ações permitidas e controles de acesso (pag. 22)
1.36. A solução deve permitir que sejam atribuídas autorizações granulares às execuções com nível administrativo em sistemas Microsoft Windows como, por exemplo, a execução de uma ou mais aplicações com nível administrativo, sem que esse privilégio seja global.	SIM	senhasegura.go For Microsoft Windows - Objetivo (pag. 7)
1.37. A solução deve garantir a configuração de mecanismo para que as senhas randomizadas sejam únicas para cada credencial.	SIM	Carta Comercial
1.38. A solução deve garantir a configuração de mecanismo para que determinados grupos de senhas randomizadas sejam as mesmas para cada credencial pertencente a este grupo.	SIM	Operações Automatizadas - Configurar perfis de Credenciais e Dispositivos (pag. 47)
1.39. A solução deve suportar em todos seus métodos de acesso, autenticação de duplo fator compatível com os métodos a seguir:	N/A	N/A
1.39.1. Algoritmos de One-time Password;	SIM	Gestão de Usuários - Duplo fator de autenticação (pag. 46)
1.39.2. Certificado digital (x.509).	SIM	Gestão de Usuários - Configurar autenticação via certificados X.509 físicos ou virtuais (pag. 58)
1.40. A solução deve ser compatível com pelo menos 02 (dois) dos seguintes métodos e padrões de criptografia:	N/A	N/A
1.40.1. AES com chaves de 256 bits;	SIM	Especificação Técnica - Criptografia e Recursos de Segurança (pag. 24)
1.40.2. FIPS 140-2;	SIM	Especificação Técnica - Criptografia e Recursos de Segurança (pag. 24)
1.40.3. Encriptação PKCS#11 ou superior por hardware utilizando dispositivos de HSM devidamente homologados pelo fabricante para a solução ofertada;	SIM	Especificação Técnica - Criptografia e Recursos de Segurança (pag. 24)
1.41. A solução deve disponibilizar a opção de autenticação utilizando os protocolos OpenID ou SAML 2.0.	SIM	Gestão de Usuários - Configurar autenticação via SAML 2.0 (pag. 54) Gestão de Usuários - Configurar autenticação via OpenID (pag. 56)
1.42. A solução deve criptografar o banco de dados utilizado para o armazenamento das senhas e credenciais gerenciadas.	SIM	Especificação Técnica - Criptografia e Recursos de Segurança (pag. 24)
1.43. A solução deve possuir função de monitoramento e análise de comportamento para os sistemas e/ou dispositivos que contemplem, no mínimo, as especificações técnicas do parque computacional do CONTRATANTE.	SIM	Auditoria e Rastreabilidade - Análise de comportamentos (pag. 38)
1.44. A solução deve, a partir dos eventos coletados, montar perfis de comportamento dos usuários do sistema.	SIM	Auditoria e Rastreabilidade - User Posture (pag. 38)
1.45. A solução deve alertar abusos e comportamentos fora dos padrões aprendidos ou mapeados.	SIM	Auditoria e Rastreabilidade - Análise de comportamentos (pag. 38)
1.46. A solução deve monitorar e exibir acessos e atividades realizadas no próprio sistema.	SIM	Auditoria e Rastreabilidade - Análise de comportamentos (pag. 38)
1.47. A solução deve detectar pelo menos os seguintes comportamentos anormais:	N/A	N/A
1.47.1. Acessos excessivos a contas privilegiadas. Quando um usuário acessa contas privilegiadas com mais frequência do que o normal, de acordo com seu perfil comportamental;	SIM	Auditoria e Rastreabilidade - Acessos excessivos (pag. 38)
1.47.2. Alteração de senha suspeita. Quando é identificada uma solicitação para alteração ou redefinição de uma senha ignorando ação executada pela solução;	SIM	Operações Automatizadas - Garantindo a validade da senha - reconciliação de senha (pag. 32)
1.47.3. Acesso privilegiado a solução através de IP irregular/incomum ou desconhecido. Quando um usuário acessa contas privilegiadas de endereço IP e sub-rede incomum, de acordo com seu perfil comportamental. Caso a solução não possua alertas baseando- se em IP, deve ao menos limitar o acesso a credenciais através de redes desconhecias e possuir informação da origem do acesso em seus relatórios.	SIM	Auditoria e Rastreabilidade - Acessos por origem incomum (pag. 40)

1.48. As detecções da solução não devem limitar-se a um tipo específico de comportamento anormal, possibilitando a correta demonstração de eventos complexos contemplando análise de comportamento de usuários.	SIM	Auditoria e Rastreabilidade - Análise de comportamentos (pag. 38)
1.49. A solução deve fornecer, por demanda do CONTRATANTE, funcionalidade para encerramento de sessões suspeitas por sistemas de terceiros em utilização no CONTRATANTE, tais como ferramentas de SIEM, software de gerenciamento de servidores, software de gerência de Backup e SGBD.	SIM	App2App - Dashboard de ameaças (pag. 39) App2App - Encerramento compulsório de sessão proxy (pag. 34)
1.50. A solução deve permitir a configuração de eventos críticos a serem reportados automaticamente, baseados, no mínimo, em:	N/A	N/A
1.50.1. Comandos Linux;	SIM	Proxy - Registro de novos comandos (pag. 85)
1.50.2. Expressões regulares para comandos, no mínimo, em SSH;	SIM	Proxy - Registro de novos comandos (pag. 85)
1.51. A solução deve disponibilizar ao usuário acesso a console da solução, incluindo, no mínimo:	N/A	N/A
1.51.1. Acesso por interface WEB, sem necessidade de plug-in ou agente específico para o acesso;	SIM	Especificação Técnica - Compatibilidade com Browser (pag. 30)
1.51.2. Utilização de protocolos de comunicação totalmente criptografados, por exemplo TLS 1.2;	SIM	Especificação Técnica - Compatibilidade com Browser (pag. 30) Especificação Técnica - Criptografia (pag. 24)
1.51.3. Suporte ao funcionamento dentro de redes que não estão diretamente conectadas à internet;	SIM	Especificação Técnica - Condições de operação de rede (pag. 30)
1.51.4. Suporte a injeção automática de credenciais, permitindo a autenticação ou elevação de privilégios para sistemas remotos, sem revelar credenciais e senhas de texto simples. Permitindo que os usuários selecionem a credencial a ser utilizada a partir de lista de credenciais que têm privilégios nos sistemas aprovados para acesso;	SIM	Proxy - Uso do Proxy (pag. 17)
1.51.5. A injeção de senhas deve ser totalmente integrada com a solução de cofre de senhas corporativa, permitindo que seus usuários usem senhas com segurança durante as sessões de acesso;	SIM	Proxy - Uso do Proxy (pag. 17)
1.51.6. Suportar os seguintes modos de acesso a desktops, servidores e outros sistemas remotos autônomos.	N/A	N/A
1.51.6.1. Integração com RDP (Remote Desktop Protocol) da Microsoft para realizar sessões utilizando protocolo RDP;	SIM	Proxy - senhasegura RDP Proxy (pag. 44)
1.51.6.2. Acesso a dispositivos de rede habilitados para SSH/telnet;	SIM	Proxy - senhasegura Terminal Proxy (pag. 27)
1.51.6.3. Acesso a páginas WEB utilizando HTTP/HTTPS;	SIM	Proxy - senhasegura Web Proxy (pag. 54)
1.52. O equipamento da solução deve suportar retenção de gravações por 90 dias, considerando o no mínimo de 8 horas/dia, 5 dias por semana de gravações.	SIM	Carta Comercial
1.53. Deve armazenar os todos logs da solução por, no mínimo, 180 dias.	SIM	Especificação Técnica - Limite de recurso (pag. 34)
1.54. Todos os sistemas e recursos necessários para operação do módulo de cofre de senhas, incluindo seu banco de dados, deverão ser passíveis de plena utilização a partir de um único nó, em caso de contingência, seja ele virtual ou físico.	SIM	Especificação Técnica - Disponibilidade e Contingência (pag. 28)
1.55. Não deve haver cobranças à parte no licenciamento de software para opção de ambiente de suporte ativo/passivo ou ativo/ativo ou arranjos de arquitetura. físico-físico, virtual-virtual e físico-virtual.	SIM	Carta Comercial
1.56. A solução deve poder ser monitorada via software de monitoramento utilizado pelo CONTRATANTE descrito no ANEXO II - RESUMO DO AMBIENTE DE TI.	SIM	Especificação Técnica - Monitoramento e Syslog e SIEM (pag. 29) Interface Web Orbit - Monitoramento através de Zabbix (pag. 28)
1.57. A solução deve poder integrar-se sem custos adicionaiscom as soluções de Help Desk (ITSM) descritas no ANEXO II - RESUMO DO AMBIENTE DE TI.	SIM	Especificação Técnica - Ferramentas ITSM (pag. 23) Informações Privilegiadas - CA Service Desk Manager (pag. 42)
1.58. A integração com a solução de Help Desk (ITSM) deve possibilitar a verificação e garantia de que todas as solicitações de checkout das senhas de credenciais privilegiadas sejam originadas de tickets válidos existentes na solução de Help Desk.	SIM	Gestão de Usuários - Integração ITSM (pag. 37)
1.59. A solução deve integrar-se diretamente, sem codificação adicional ou adição de scripts, com soluções de SIEM, a fim de garantir o registro e a visualização, a partir da aplicação existente nesses sistemas, das seguintes ações, no mínimo:	N/A	N/A
1.59.1. Atividades administrativas relacionada a acesso as credenciais privilegiadas;	SIM	Monitoramento e Notificações - Mensagens configuradas (pag. 16)
1.59.2. Atividades de recuperação, liberação e alterações de senhas;	SIM	Monitoramento e Notificações - Mensagens configuradas (pag. 16)
1.59.3. Outras atividades de executadas pelos usuários na console web;	SIM	Monitoramento e Notificações - Mensagens configuradas (pag. 16)
1.60. A solução deve utilizar um banco de dados com as melhores práticas de segurança, em ambiente “hardenizado”, com mecanismo de blindagem e criptografia do sistema operacional.	SIM	Especificação Técnica - Criptografia (pag. 24)
1.61. Os appliances e sistemas operacionais da solução devem ser “hardenizados” e protegidos com firewall interno e sistema detecção de intrusão ou solução de proteção contra ameaças.	SIM	Interface Web Orbit - Bloqueio HIDS (Wazuh) (pag. 26)
1.62. Caso a solução utilize sistema operacional de terceiros, este deverá vir licenciado para a proteção interna do appliance e aplicação.	SIM	Especificação Técnica - Sistemas básicos componentes da solução (pag. 6)

1.63. A solução deve utilizar uma arquitetura de banco de dados e aplicação que permita alta disponibilidade e mecanismos para a recuperação de desastres para todos os componentes da solução.	SIM	Interface Web Orbit - Alta Disponibilidade (HA) e Recuperação de Desastre (DR) (pag. 45)
1.64. A solução deve permitir o backup e restore de seu banco de dados, bem como das configurações de software estabelecidas, com as seguintes capacidades:	N/A	N/A
1.64.1. Permitir a execução de tarefas de backup criptografado sem a necessidade de agentes de terceiros ou parada do ambiente ou comprometimento de qualquer funcionalidade; provendo assim o maior nível possível de segurança e integridade dos dados a serem copiados;	SIM	Interface Web Orbit - Configurando e utilizando o Backup (pag. 40)
1.64.2. Permitir a execução de backups automatizados, permitindo a programação/agendamento de horários e configuração de locais para seu armazenamento local e remoto;	SIM	Interface Web Orbit - Pré-requisitos para configuração (pag. 41)
1.65. Caso a solução faça uso de mecanismos para controle e otimização da carga de trabalho interna, de modo a possibilitar o controle de parâmetros, melhorar ou ajustar o seu desempenho de acordo com as características do ambiente onde está localizado, estes mecanismos deverão ser providos pela solução.	SIM	Interface Web Orbit - Tuning do servidor (pag. 27)
1.66. A solução deve ser capaz de exportar a chave de criptografia ou credencial equivalente do local de armazenamento das credenciais (cofre), por meio de backup ou método análogo, para ser utilizada nos cenários de recuperação de desastres, de forma a conceder acesso à todas as senhas de identidades privilegiadas e dados gerenciados pela solução.	SIM	Chave Mestra - A Chave Mestra (pag. 3)
1.67. O acesso primário dos usuários à solução deve ser sempre a partir dos componentes instalados em sua rede local.	SIM	Interface Web Orbit - Configurando a Alta Disponibilidade (pag. 54)
1.68. A solução deve suportar, sem necessidade de licenciamento adicional a gestão de senhas no código fonte em aplicações e scripts (AAPM) através de uma REST.	SIM	App2App - Integração via Webservice (pag. 5)
1.69. A solução deve suportar API REST, onde as aplicações consomem a senha com requisições a interface API REST, assim evitando que as senhas fiquem expostas no código fonte das aplicações.	SIM	App2App - Integração via Webservice (pag. 5)
1.70. A solução deve permitir o envio automático de logs para servidores Syslog de forma aderente ao disposto na RFC 5424 (the Syslog Protocol).	SIM	Monitoramento e Notificações - Syslog (pag. 7)
1.71. As solução deve permitir a definição de fluxos de aprovação (workflows) para obtenção de acesso às contas privilegiadas, com as seguintes características:	N/A	N/A
1.71.1. Personalização da configuração de fluxos para aprovação, de acordo com a criticidade e características da conta (como de acesso emergencial, de uso por terceiros), e aprovação de pelo menos um responsável;	SIM	Informações Privilegiadas - Workflow de acesso (pag. 32)
1.71.2. Aprovação perante agendamento de ações administrativas, ou seja, a aprovação do acesso ocorrera em um dia, mas a liberação da senha ocorrerá de forma automática somente na data e horário previstos;	SIM	Informações Privilegiadas - Acesso através de aprovação (pag. 33)
1.71.3. Substituição de senhas de identidades privilegiadas em uso por determinado serviço ou por tarefa agendada em todos os locais onde estejam sendo utilizadas;	SIM	Operações Automatizadas - Operação encadeada usando esquema de credencial pai e filha (pag. 14)
1.71.4. Caso seja necessário, após alteração da senha de identidade privilegiada associada à um serviço, a solução deve ser capaz de reinicializar o mesmo.	SIM	Operações Automatizadas - Registrando um template (pag. 17)
1.72. A solução deve permitir o agrupamento lógico de sistemas a fim de simplificar a configuração de políticas apropriadas para diferentes tipos de sistemas alvo. Além de permitir a atualização de uma mesma conta em múltiplos sistemas-alvo com uma única tarefa de alteração de senhas.	SIM	Operações Automatizadas - Configurar perfis de Credenciais e Dispositivos (pag. 47)
1.73. A solução deve ser capaz de redefinir senhas individuais ou grupos de senhas sob demanda e deve ser capaz de realizar verificações agendadas e automáticas a fim de garantir que as senhas das contas gerenciadas pela solução no dispositivo de destino, correspondam às mesmas senhas armazenadas no banco de dados da solução.	SIM	Operações Automatizadas - Configurar perfis de Credenciais e Dispositivos (pag. 47) Operações Automatizadas - Garantindo a validade da senha - reconciliação de senha (pag. 32)
1.74. A solução deve ser capaz de descobrir e alterar credenciais Microsoft Windows, incluindo contas nomeadas, administradores 'built-in' e convidados, exibindo em mapa de rede gráfico e interativo ou através de relatórios e interface de gerenciamento.	SIM	Scan & Discovery - Visualizar credenciais (pag. 43)
1.75. A solução deve ser capaz descobrir e alterar credenciais privilegiadas em ambientes Linux e Unix.	SIM	Scan & Discovery - Visualizar credenciais (pag. 43)
1.76. A solução deve identificar as contas privilegiadas com UID 0 (zero) em Linux e Unix e as contas privilegiadas através do uso do comando sudo.	SIM	Scan & Discovery - Visualizar credenciais (pag. 43)
1.77. A solução deve possibilitar a descoberta e alteração de contas privilegiadas usadas em serviços WEB de forma automática ou através de adaptações via script integrados ao SDK ou API da solução. Ex: aplicações baseadas em Microsoft IIS.	SIM	Scan & Discovery - Contas em pool de aplicações IIS (pag. 52)
1.78. A solução deve descobrir e alterar processos interdependentes e credenciais de serviço, incluindo credenciais em ambientes clusterizados.	SIM	Scan & Discovery - Credenciais associadas a serviços (pag. 50)

1.79. A solução deve ser capaz de encontrar contas de usuários privilegiados que possam ser gerenciadas pela solução, permitindo que a conta descoberta seja gerenciada pela solução.	SIM	Scan & Discovery - Importar credenciais encontradas (pag. 38)
1.80. A solução deve ser capaz de substituir as senhas de identidades privilegiadas que estejam sendo utilizadas por determinado serviço em todos os locais onde estejam sendo utilizadas.	SIM	Operações Automatizadas - Configuração de execução (pag. 26)
1.81. A solução deve ser capaz de realizar discovery automatizado de credencias em servidores e bancos de dados.	SIM	Scan & Discovery - Sobre o módulo (pag. 6)
1.82. A descoberta automática de credenciais da solução deve ser realizada por buscas no Active Directory (AD) e/ou por ranges de endereços IP.	SIM	Scan & Discovery - Criando um Scan do tipo Domínio (pag. 12) Scan & Discovery - Criando um Scan do tipo Dispositivos (pag. 14)
1.83. A solução deve descobrir e alterar credenciais do Active Directory (AD) e todos os outros serviços de diretório compatíveis com LDAP.	SIM	Scan & Discovery - Criando um Scan do tipo Domínio (pag. 12) Operações Automatizadas - LDAP (pag. 59)
1.84. O gerenciamento de identidades privilegiadas deverá disponibilizar:	N/A	N/A
1.84.1. Mecanismo de retirada e devolução de contas e senhas compartilhadas;	SIM	Informações Privilegiadas - Políticas de Credenciamento (pag. 69) Informações Privilegiadas - Auditoria (pag. 74)
1.84.2. Definição de tempo de validade: permitir o estabelecimento de tempo de validade para as senhas de identidades privilegiadas gerenciadas que forem requisitadas;	SIM	Informações Privilegiadas - Políticas de Credenciamento (pag. 69)
1.84.3. Troca automática da senha no sistema gerenciado, após a sua devolução ou após o vencimento do tempo de validade estabelecido;	SIM	Informações Privilegiadas - Políticas de Credenciamento (pag. 69)
1.84.4. Configuração de calendário de requisição de senhas de identidades privilegiadas com base em usuários ou grupos de usuários;	SIM	Informações Privilegiadas - Acesso através de aprovação (pag. 33)
1.84.5. Troca de Senhas por Demanda: Permitir a troca de senhas nos Sistemas Gerenciados, de forma individual ou por grupos customizáveis, manualmente ou de forma automática, por agendamento.	SIM	Operações Automatizadas - Solicitando uma troca (pag. 30)
1.85. No processo de definição da política de composição de senha, a solução deve ser capaz de:	N/A	N/A
1.85.1. Gerar senhas aleatórias com extensão de 128 (cento e vinte e oito) caracteres ou mais.	SIM	Informações Privilegiadas - Força da senha (pag. 66)
1.85.2. Utilizar caracteres alfabéticos (maiúsculos e minúsculos), numéricos e símbolos.	SIM	Informações Privilegiadas - Força da senha (pag. 66)
1.85.3. Especificar qual o tipo de caractere na composição das senhas a serem geradas;	SIM	Informações Privilegiadas - Força da senha (pag. 66)
1.85.4. Permitir a determinação de quais símbolos estão excluídos ou exclusivamente permitidos na composição da senha;	SIM	Informações Privilegiadas - Força da senha (pag. 66)
1.85.5. Garantir a configuração de mecanismo para que as senhas randomizadas sejam únicas para cada credencial;	SIM	Carta Comercial
1.85.6. Garantir a configuração de mecanismo para que determinados grupos de senhas randomizadas sejam as mesmas para cada credencial pertencente a este grupo;	SIM	Operações Automatizadas - Configurar perfis de Credenciais e Dispositivos (pag. 47)
1.85.7. Implementar controle de acesso baseado em papéis (roles), garantindo aderência ao princípio dos privilégios mínimos, e viabilizando a segregação de funções entre usuários de uma mesma aplicação gerenciada.	SIM	Gestão de Usuários - Camada de Controle de Acesso senhasegura (pag. 7)
1.86. A solução não deverá permitir a abertura do cofre com chaves criptográficas geradas por seus respectivos fornecedores e/ou fabricantes.	SIM	Chave Mestra - A Chave Mestra (pag. 3)
1.87. Deve 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.	SIM	Auditoria e Rastreabilidade - Rastreabilidade (pag. 15)
1.88. Todas as sessões acessadas no cofre digital devem ser gravadas, possibilitando a visualização destes vídeos na solução, com opção de armazenamento externo dos vídeos para que seja possível guardá-los por tempo indeterminado caso seja necessário.	SIM	Proxy - Logs e vídeos das sessões (pag. 71)
1.89. As sessões acessadas por usuários poderão ser monitoradas pelo administrador da solução, o qual poderá bloquear e/ou interromper o acesso a qualquer tempo. Caso ocorra o bloqueio e/ou interrupção, estas ações exercidas pelo administrador também deverão ser gravadas.	SIM	Proxy - Ações durante uma sessão (pag. 10)
1.90. A solução deve 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.	SIM	Informações Privilegiadas - Acesso através de aprovação (pag. 33)
1.91. A solução deve filtrar comandos executados ao longo das sessões gravadas, possibilitando pesquisar ações específicas nos vídeos gravados.	SIM	Proxy - Comandos auditados (pag. 83)
1.92. A pesquisa textual deve remeter ao momento exato em que o texto ou comando foi realizado no vídeo da gravação da sessão.	SIM	Proxy - Registros e Execuções de Comando (pag. 93)

1.93. A solução deve permitir que os comandos executados em sistemas Linux e Unix monitorados sejam gravados em modo texto.	SIM	Proxy - Textos centralizados indexados (pag. 74)
1.94. Deve ser possível colocar a sessão em quarentena ficando pendente de liberação e terminação pelo administrador ou permitir o monitoramento da sessão em tempo real permitindo sua terminação pelo administrador.	SIM	Proxy - Ações durante uma sessão (pag. 10)
1.95. Deve possibilitar assistir o vídeo de uma sessão diretamente na solução, sem necessidade de converter em formato de vídeo ou realizar download.	SIM	Proxy - Logs para uma sessão (pag. 72)
1.96. Deve possibilitar sessões remotas através de programas instalados na estação de trabalho do cliente, a exemplo do Putty e RDP Client, sem obrigatoriedade de passar pela aplicação WEB ou baixar cliente adicional.	SIM	Proxy - senhasegura Terminal Proxy (pag. 27) Proxy - senhasegura RDP Proxy (pag. 44)
1.97. Deve permitir a inclusão de comentários em sessões gravadas, e marcar sessões como já revistas.	SIM	Proxy - Solicitação de auditoria (pag. 79)
1.98. Conceder acesso aos sistemas utilizando "Remote Desktop" e "SSH" sem que os usuários vejam qualquer senha, garantindo que não haja necessidade de instalação de aplicações e/ou agentes nas estações dos usuários para realizar o acesso, devendo conceder acesso a:	N/A	N/A
1.98.1. Sistemas ou aplicações parametrizáveis, onde a aplicação deverá ser executada, por meio de página web, devidamente autenticada com usuário e senha pré-determinados ou recuperados da base de dados da solução, sem que haja login interativo por parte dos usuários no sistema operacional do servidor de destino, possibilitando habilitar gravação da sessão caso seja necessário. Exemplo: Executar o SQL Management Studio com credencial de SA (System Administrator) sem que o usuário conheça a senha e sem necessidade de login interativo prévio do usuário no sistema operacional do host de destino;	SIM	Proxy - SSH RemoteApp (pag. 38) Proxy - RDP RemoteApp (pag. 65)
1.98.2. Sistemas baseados em Remote Desktop e SSH sem que os usuários vejam a senha. A senha vigente no momento (estática ou dinâmica) deverá ser provida para as aplicações ou conexões remotas devendo ser recuperadas de forma automática e transparente do banco de dados da solução.	SIM	Proxy - senhasegura Terminal Proxy (pag. 27) Proxy - senhasegura RDP Proxy (pag. 44)
1.98.3. As sessões acessadas podem ser monitoradas por meio de gravação de vídeos das mesmas, em formato padrão de execução da solução;	SIM	Proxy - Logs para uma sessão (pag. 72)
1.98.4. A solução deve permitir que um administrador possa bloquear e desbloquear, e terminar uma sessão ativa caso julgue necessário.	SIM	Proxy - Ações durante uma sessão (pag. 10)
1.98.5. Monitorar comandos executados ao longo da sessão gravada, possibilitando pesquisar ações específicas no vídeo gravado.	SIM	Proxy - Registros e Execuções de Comando (pag. 93)
1.98.6. A solução deve possuir a opção de terminar a sessão automaticamente em uma sessão SSH se o usuário digitar um comando não autorizado.	SIM	Proxy - Ações acionadas pela execução de comandos auditados (pag. 84)
1.98.7. A solução deve permitir que as sessões SSH e RDP abertas através da solução sejam terminadas de forma automática ao expirar o tempo requisitado de sessão.	SIM	Informações Privilegiadas - Acesso através de aprovação (pag. 33)
1.98.8. A solução deve suportar forçar o logoff dos usuários em sessões RDP terminadas pela solução ao final do tempo de requisição da sessão.	SIM	Informações Privilegiadas - Acesso através de aprovação (pag. 33)
1.99. A solução deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução, tais como:	N/A	N/A
1.99.1. Lista de sistemas gerenciados;	SIM	Informações Privilegiadas - O relatório de dispositivos (pag. 7)
1.99.2. Senhas armazenadas;	SIM	Auditoria e Rastreabilidade - Listagem geral (pag. 26)
1.99.3. Eventos de alteração de senha;	SIM	Auditoria e Rastreabilidade - Credenciais (pag. 17)
1.99.4. Auditoria de contas;	SIM	Auditoria e Rastreabilidade - Credenciais (pag. 17)
1.99.5. Auditoria de sistemas;	SIM	Auditoria e Rastreabilidade - Dispositivos (pag. 18)
1.99.6. Auditoria de usuários;	SIM	Auditoria e Rastreabilidade - Audit tracking (pag. 25)
1.99.7. Detalhes das próximas atualizações de senha programadas;	SIM	Auditoria e Rastreabilidade - Expiração das senhas (pag. 8)
1.99.8. Sistemas que estão usando uma conta de serviço para iniciar um ou mais serviços;	SIM	Scan & Discovery - Credenciais associadas a serviços (pag. 50)
1.100. A solução deve controlar o acesso aos relatórios se baseando nas permissões configuradas na solução.	SIM	Gestão de Usuários - Camada de Controle de Acesso senhasegura (pag. 7)
1.101. 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.	SIM	Auditoria e Rastreabilidade - Dashboards (pag. 34)
1.102. 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.	SIM	Interface Gráfica do Usuário - Tela típica de relatório (pag. 20)
1.103. A solução deve fornecer relatórios de auditoria que disponibilizem detalhes das interações dos usuários com a solução, tais como:	N/A	N/A
1.103.1. Auditoria detalhada, com no mínimo, atividade de login e logoff dos usuários;	SIM	Auditoria e Rastreabilidade - Histórico de acessos (pag. 21)

1.103.2. Alterações nas funções de delegação;	SIM	Auditoria e Rastreabilidade - Histórico de permissões e papéis (pag. 34)
1.103.3. Adições, deleções, alterações de senhas gerenciadas pela solução;	SIM	Auditoria e Rastreabilidade - Credenciais (pag. 17)
1.103.4. Operações das senhas dos usuários, incluindo check-in e checkout, solicitações negadas e permitidas;	SIM	Auditoria e Rastreabilidade - Vizualização de senhas (pag. 23) Informações Privilegiadas - Solicitações de acesso (pag. 32)
1.103.5. Os relatórios devem ser filtrados por período de tempo, tipo de operação, sistema, gerente e assim por diante.	SIM	Interface Gráfica do Usuário - Tela típica de relatório (pag. 20)
1.104. A solução deve possibilitar a geração de relatórios, no mínimo, em um dos formatos a seguir:	N/A	N/A
1.104.1. Formato editável: HTML, CSV, XLSX ou XLS.	SIM	Especificação Técnica - Relatórios (pag. 11) Interface Gráfica do Usuário - Tela típica de relatório (pag. 20)
1.104.2. Formato não editável: PDF	SIM	Especificação Técnica - Relatórios (pag. 11) Interface Gráfica do Usuário - Tela típica de relatório (pag. 20)
2. Módulo - Elevação de Privilégios Servidores Linux	N/A	N/A
2.1. O módulo de elevação de privilégios de servidores Linux deve ser licenciado de forma a atender o quantitativo mínimo de 230 (duzentos e trinta) dispositivos.	SIM	Carta Comercial
2.2. Deve ser capaz de garantir o controle, elevação de privilégios e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino fazendo uso de agente instalado no sistema ou método análogo.	SIM	senhasegura.go for Linux - Introdução (pag. 3)
2.3. Deve deve implementar um modelo de delegação de privilégios mínimos, permitindo que os usuários executem qualquer comando em um nível de privilégio mais alto, desde que permitido pela política centralizada e removendo a necessidade de os usuários efetuarem logon como root.	SIM	senhasegura.go for Linux - Cadastrando diretivas a nível de kernel (pag. 10)
2.4. Deve ser capaz de limitar o acesso a contas privilegiadas, permitindo que um usuário execute determinadas tarefas em um servidor Linux e Unix, sem dar acesso a contas privilegiadas, fazendo uso de agente instalado no sistema ou método análogo.	SIM	senhasegura.go for Linux - Introdução (pag. 3)
2.5. Deve prover um controle de comandos completo, possuindo a possibilidade de criar uma lista de comandos permitidos ou bloqueados (whitelisting/blacklisting), lista de comandos a serem alterados (criação de alias) ou prevenir que comandos sejam executados.	SIM	senhasegura.go for Linux - Alias de comando (pag. 12)
2.6. Deve prover meios de permitir que os usuários executem comandos específicos e conduzam sessões remotamente baseado em regras sem autenticar-se diretamente utilizando credenciais privilegiadas.	SIM	senhasegura.go for Linux - Prevenção de execução de binários em shell script (pag. 13)
2.7. Deve permitir que os usuários executem comandos específicos e conduzam sessões remotamente com base em regras sem fazer logon como administrador ou root.	SIM	senhasegura.go for Linux - Cadastrando diretivas a nível de kernel (pag. 10)
2.8. A política de acesso dinâmico permitirá que o administrador especifique:	N/A	N/A
2.8.1. Quais tarefas um usuário ou grupo de usuários pode executar.	SIM	senhasegura.go for Linux - Cadastrando diretivas a nível de kernel (pag. 10)
2.8.2. De qual máquina o usuário pode iniciar uma solicitação para executar a tarefa.	SIM	senhasegura.go for Linux - Cadastrando diretivas a nível de kernel (pag. 10)
2.8.3. Em quais máquinas uma tarefa pode ser executada;	SIM	senhasegura.go for Linux - Cadastrando diretivas a nível de kernel (pag. 10)
2.9. Deve ser capaz de interceptar as chamadas da biblioteca relacionadas ao sistema de arquivos e permitir, proibir e auditar as chamadas. Deve permitir especificar ações (por exemplo, abrir/ler/ gravar/executar) que podem ou não ser executadas em um arquivo (usando padrões de arquivos no estilo de shell para corresponder aos arquivos) e também especificar um nível de auditoria;	SIM	senhasegura.go for Linux - Controle de diretórios e arquivos (pag. 18)
2.10. Deve ser capaz de controlar, bloquear e auditar comandos executados em um script quando ele é elevado pela solução, mesmo como root;	SIM	senhasegura.go for Linux - Prevenção de execução de binários em shell script (pag. 13) senhasegura.go for Linux - Gravação de sessão (pag. 17)
2.11. Deve fornecer shells baseadas nas variantes Bourne e Korn de domínio público e fornecer os seguintes recursos:	N/A	N/A
2.11.1.Autorização transparente para cada comando, redirecionamento e comando interno;	SIM	senhasegura.go for Linux - Cadastrando diretivas a nível de kernel (pag. 10)
2.11.2.Controle de scripts de shell;	SIM	senhasegura.go for Linux - Cadastrando diretivas a nível de kernel (pag. 10)
2.11.3.Log de Entrada / Saída para toda a sessão de shell ou para comandos seletivos;	SIM	senhasegura.go for Linux - Relatório de eventos (pag. 19) senhasegura.go for Linux - Logs de comandos (pag. 20)
2.11.4.Registro de eventos para cada comando, redirecionamento e comando interno;	SIM	senhasegura.go for Linux - Alias de comando (pag. 12) senhasegura.go for Linux - Logs de comandos (pag. 20)
2.12. Deve fornecer registro básico que registre as seguintes informações: data/hora do evento, status de aceitação e rejeição, eventos de ação de pressionamento de tecla, status da tarefa, comando que o usuário solicitou, comando executado, e o usuario que executou o comando, mesmo em casos de usuario executando comando como root.	SIM	senhasegura.go for Linux - Logs de comandos (pag. 20)

2.13. Deve fornecer log de comandos pré-configurados ou de toda a sessão que podem ser guardados e permitindo sua reprodução como um vídeo de todos os comandos executados localmente no servidor.	SIM	senhasegura.go for Linux - Gravação de sessão (pag. 16)
2.14. Deve se integrar a ferramentas de SIEM para enviar dados do evento Aceitos e Rejeitados via Syslog.	SIM	Monitoramento e Notificações - SIEM (pag. 5)
2.15. Deve ser capaz de criptografar todo o tráfego de rede gerado, incluindo mensagens de controle, entrada que é digitada pelos usuários e saída gerada pelos comandos que são executados através dela.	SIM	senhasegura.go for Linux - Preparando o senhasegura para receber o disposito alvo (pag. 4)
2.16. Deve ser capaz de se integrar a ferramentas de HSM para usar os serviços de criptografia FIPS 140-2 Security Level 2 para obter conformidade com os requisitos e padrões de armazenamento de chaves mais rigorosos.Deve suportar criptografia segura de log.	SIM	Especificação Técnica - Criptografia com HSM (pag. 24)
2.17. Deve fornecer painéis e relatórios gerenciais.	SIM	Auditoria e Rastreabilidade - go (pag. 37)
3. Módulo - Elevação de Privilégios Servidores Microsoft Windows	N/A	N/A
3.1. O módulo de elevação de privilégios de servidores Windows deve ser licenciado de forma a atender o quantitativo mínimo de 90 (noventa) dispositivos.	SIM	senhasegura.go Windows - O senhasegura.go (pag. 7)
3.2. Deve possuir agente local para Servidores Microsoft Windows que permita a remoção do privilégio administrativo dos usuários, permitindo a elevação de privilégios através de regras pré-definidas.	SIM	senhasegura.go Windows - O senhasegura.go (pag. 7)
3.3. Deve possuir mecanismos para fazer a elevação de privilégios de aplicações autorizadas no Microsoft Windows, a fim de atribuir o direito de administrador somente as tarefas autorizadas para cada tipo de usuário (mesmo que o mesmo não tenha direitos de administrador) e implementar a segregação de funções.	SIM	senhasegura.go Windows - Regras denylist e allowlist (pag. 46)
3.4. Deve permitir a criação regras de privilégios, onde o privilégio de administrador é concedido para cada aplicativo/processo autorizado, de forma que cada usuário, mesmo com o privilégio de usuário convencional (usuário standard) possa instalar certos programas permitidos, possa executar os aplicativos legados que requerem o privilégio de administrador para funcionar, controles ActiveX, etc.	SIM	senhasegura.go Windows - Regras denylist e allowlist (pag. 46)
3.5. Deve permitir a remoção de direitos de administração local dos usuários e grupos de maneira segmentada.	SIM	senhasegura.go Windows - O senhasegura.go (pag. 7)
3.6. Deve suportar que os aplicativos sejam agrupados logicamente em vez de criar uma regra para cada aplicativo. Estes grupos de aplicativos devem permitir sua reutilização em diferentes políticas.	SIM	senhasegura.go Windows - Regras denylist e allowlist (pag. 46) Aplicações: Segregações de aplicações ou grupo de aplicações que farão ...
3.7. Deve permitir criar uma lista branca (whitelist), onde seja possível configurar todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista automaticamente seja bloqueada.	SIM	senhasegura.go Windows - Regras denylist e allowlist (pag. 46)
3.8. Caso a solução permita a execução dos aplicativos em lista branca (whitelist) sem escaneamento prévio por solução de segurança do CONTRATANTE, a solução deverá prover função de descoberta de malware em cada processo em execução, através da comparação automática do hash com fabricantes de antivírus (integração com virustotal) sem que o administrador precise executar a submissão manual.	SIM	senhasegura.go Windows - Detecção de atividade maliciosa (pag. 62)
3.9. Deve permitir, caso configurado, que um usuário faça o clique com o botão direito do mouse e possa executar uma aplicação com direitos de administrador, sem ter que saber a senha da conta local administrador (privilégio sob demanda, com justificativas)	SIM	senhasegura.go Windows - Elevando um aplicativo fora do senhasegura.go (pag. 26)
3.10. Deve possuir uma integração com Controle de Conta de Usuário do Microsoft Windows (UAC).Todas as políticas dever ser mantidas em cache e serem aplicadas ao endpoint mesmo que o mesmo não esteja conectado à rede corporativa.	SIM	senhasegura.go Windows - Integração com UAC (pag. 48)
3.11. Deve suportar a elevação segura de tipos de arquivos hospedados, como o Microsoft Management Consoles (MMC), sem depender de linha de comandos.	SIM	senhasegura.go Windows - Realizando uma elevação de privilégio (pag. 24)
3.12. Deve suportar a elevação de scripts aprovados, incluindo scripts do tipo “Batch Files”, scripts do Microsoft Windows e Microsoft PowerShell.	SIM	senhasegura.go Windows - Realizando uma elevação de privilégio (pag. 24)
3.13. Deve permitir elevação de scripts e comandos individuais do Microsoft PowerShell ou bloqueio de execução da aplicação do CMD executados em uma máquina remota.	SIM	senhasegura.go Windows - Controle de comandos executados (pag. 60)
3.14. Deve possuir auditoria granular de todas as atividades remotas.	SIM	senhasegura.go Windows - Relatório de eventos (pag. 37)
3.15. Deve evitar que anexos de e-mail maliciosos ou documentos baixados iniciem executáveis desconhecidos que possam infectar o sistema do cliente e criptografar dados dos usuários.	SIM	senhasegura.go Windows - Regras denylist e allowlist (pag. 46)
3.16. Deve impedir que processos ou executáveis desconhecidos executados a partir de um site devem ser impedidos de serem executados.	SIM	senhasegura.go Windows - Regras denylist e allowlist (pag. 46)
3.17. Deve impedir que quando o usuário abre uma sessão do navegador ou manipuladores de documentos, como o Microsoft Office ou o Adobe Reader, os processos desconhecidos não devem ter permissão para acessar e adulterar dados privados.	SIM	senhasegura.go Windows - Controle de diretórios e arquivos (pag. 58)
3.18. Deve forçar que conteúdo não confiável não deve poder fazer modificações no sistema operacional, no registro e nos aplicativos instalados.	SIM	senhasegura.go Windows - Controle de diretórios e arquivos (pag. 58)

3.19. Através de regras pré-definidas, deve forçar que quando um usuário abre um navegador ou um manipulador de documentos, somente os processos confiáveis e processos filho devem ser permitidos, e qualquer aplicativo potencialmente mal-intencionado será impedido de iniciar.	SIM	senhasegura.go Windows - Detecção de atividade maliciosa (pag. 62)
3.20. Deve permitir que mensagens customizadas sejam mostradas antes que uma aplicação seja executada ou bloqueada.	SIM	senhasegura.go Windows - Configurações globais (pag. 38)
3.21. Deve consolidar os logs a soluções de SIEM para correlação e notificação de eventos.	SIM	Monitoramento e Notificações - SIEM (pag. 5)
3.22. Deve identificar o uso de aplicativos e a tentativa de uso, incluindo aplicativos bloqueados e restritos.	SIM	senhasegura.go Windows - Relatório de eventos (pag. 37)
3.23. Deve relacionar os aplicativos instalados fornecendo informações sobre implantação e uso de políticas.	SIM	senhasegura.go Windows - Modo de aprendizado (pag. 63)
3.24. Deve fornecer painéis e relatórios gerenciais.	SIM	Auditoria e Rastreabilidade - go (pag. 37)
4. Módulo - Elevação de Privilégios em Estações de Trabalho (Desktops)	N/A	N/A
4.1. O módulo de elevação de privilégios de desktops Windows e Linux deve ser licenciado de forma a atender o quantitativo mínimo de 50 (cinquenta) desktops Windows e 10 (dez) desktops Linux.	SIM	Carta Comercial
4.2. Deve possuir mecanismos para fazer a elevação de privilégios de aplicações autorizadas no Microsoft Windows, a fim de atribuir o direito de administrador somente as tarefas autorizadas para cada tipo de usuário (mesmo que o mesmo não tenha direitos de administrador) e implementar a segregação de funções.	SIM	senhasegura.go Windows - Regras denylist e allowlist (pag. 46)
4.3. Deve permitir a criação de regras de privilégios, onde o privilégio de administrador é concedido para cada aplicativo/processo autorizado, de forma que cada usuário, mesmo com o privilégio de usuário convencional (usuário standard) possa instalar certos programas permitidos, possa executar os aplicativos legados que requerem o privilégio de administrador para funcionar, controles ActiveX, etc.	SIM	senhasegura.go Windows - Regras denylist e allowlist (pag. 46)
4.4. Deve possuir uma integração com Controle de Conta de Usuário do Microsoft Windows (UAC).	SIM	senhasegura.go Windows - Integração com UAC (pag. 48)
4.5. Deve permitir criar uma lista branca (whitelist), onde seja possível configurar todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista automaticamente seja bloqueada.	SIM	senhasegura.go Windows - Regras denylist e allowlist (pag. 46)
4.6. Caso a solução permita a execução dos aplicativos em lista branca (whitelist) sem escaneamento prévio por solução de segurança do CONTRATANTE, a solução deverá prover função de descoberta de malware em cada processo em execução, através da comparação automática do hash com fabricantes de antivírus (integração com virustotal) sem que o administrador precise executar a submissão manual.	SIM	senhasegura.go Windows - Detecção de atividade maliciosa (pag. 62)
4.7. Deve manter as políticas em cache e aplicadas ao desktop mesmo que os desktop não esteja conectado à rede corporativa.	SIM	senhasegura.go Windows - O modo offline (pag. 47)
4.8. Deve permitir elevação de scripts e comandos individuais do Microsoft PowerShell ou bloqueio de execução da aplicação do CMD executados em uma máquina remota.	SIM	senhasegura.go Windows - Realizando uma elevação de privilégio (pag. 24)
4.9. Deve fornecer proteção de grupos de usuários privilegiados em cada estação, o que significa que os usuários não podem adulterar ou modificar grupos privilegiados locais, como o grupo Administradores ou Power Users.	SIM	senhasegura.go Windows - Regras denylist e allowlist (pag. 46)
4.10. Deve permitiro mapeamento de compartilhamento de rede com usuário diferente do usuário logado na estação.	SIM	senhasegura.go Windows - Acesso a pastas compartilhadas (pag. 28)
4.11. Deve fornecer painéis e relatórios gerenciais.	SIM	Auditoria e Rastreabilidade - go (pag. 37)

8 de dezembro, 2021

Ao,

Conselho de Justiça Federal

EDITAL Nº 37/2021
PROCESSO ADMINISTRATIVO: 0004481-11.2020.4.90.8000

Prezados Senhores,

A MT4 TECNOLOGIA LTDA., pessoa jurídica de direito privado inscrita no CNPJ sob n o 04.626.836/0001-57, com sede na Rua Joaquim Antunes, 767, conjunto 66, Pinheiros, São Paulo/SP, vem, por meio deste, declarar que a solução apresentada é totalmente aderente aos itens do edital em epígrafe indicados abaixo:

1.1. A solução de cofre de senhas deve ser licenciada de forma a atender os quantitativos mínimos descritos a seguir:
1.1.1. Quantidade de servidores Linux: 600;
1.1.2. Quantidade de servidores Microsoft Windows: 150;
1.1.3. Quantidade de estações de trabalho Microsoft Windows: 550;
1.1.4. Quantidade de estações de trabalho Linux: 30;
1.1.5. Quantidade de ativos de rede (switches, roteadores, firewalls, controladores, balanceadores, WAF e outros): 40;
1.1.6. Quantidade de instâncias de bancos de dados: 25;
1.1.7. Quantidade de licenças para cofre de senhas: 40 usuários ou 1395 dispositivos;
1.1.8. Quantidade de aplicações com senha de banco de dados armazenada localmente: 15.
1.5. A solução deve contemplar a expansão, incremento ou melhoria dos métodos utilizados para alta disponibilidade sem qualquer custo adicional de licenciamento da solução para o CONTRATANTE.
1.22. A solução, em um dispositivo licenciado, deve contemplar sua expansão, incremento ou melhoria sem qualquer custo adicional de licenciamento da solução para o CONTRATANTE.
1.23. A solução deve permitir a opção de implementar o gerenciamento de troca de senhas em redes separadas e dispositivos remotos.

Prestadas as informações, desde já nos colocamos à disposição para quaisquer esclarecimentos que entendam necessários.

Cordialmente

DocuSigned by:
Marcus Vinicius Scharra de Oliveira Paula
02DD7334A2B84D2...

Marcus Vinicius Scharra de Oliveira Paula
CEO
MT4 Tecnologia Ltda- senhasegura

8 de dezembro, 2021

Caro destinatário,

Conselho de Justiça Federal

EDITAL Nº 37/2021

PROCESSO ADMINISTRATIVO: 0004481-11.2020.4.90.8000

A quem possa interessar,

Assunto: Declaração de credenciamento como parceiro para comercialização da solução e prestação de suporte

Este documento confirma que empresa ARVVO TECNOLOGIA, CONSULTORIA E SERVICOS LTDA, localizada em: SHN QD.01 BL A SALA 1.114 E 1.115, ED. LE QUARTIER, C.E.P: 70.701-010, Brasília/DF, CNPJ/MF 25.359.140/0001-81, é parceiro MT4 Tecnologia - Senhasegura.

ARVVO TECNOLOGIA, CONSULTORIA E SERVICOS LTDA – LTDA atendeu os requerimentos da parceria Senhasegura estando apto a permanecer como membro, reconhecendo a sua demonstração de proficiência na solução solicitada, estando devidamente autorizada a comercializar, instalar, configurar e a prestar serviços de assistência técnica on-site, bem como prestar serviços de garantia técnica para os produtos e serviços constantes dessa licitação em todo território nacional.

A Confirmação é a partir da data de hoje, 08 de Dezembro de 2021.

Válida por até 90 dias.

DocuSigned by:
Marcus Vinicius Scharra de Oliveira Paula
02DD7334A2B84D2...

Marcus Vinicius Scharra de Oliveira Paula
CEO
MT4 Tecnologia Ltda- senhasegura