GOVERNO DO ESTADO DO RIO DE JANEIRO / CENTRO DE TECNOLOGIA DE INFORMAÇÃO
Rio de Janeiro, Brazil
Ref: PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOS Nº. 007/2025

To whom it may concern,

Re: Authorization of Blue Eye Soluções em Tecnologia to resell CyberArk products and services

CyberArk hereby confirms that at the date of signature of this letter Blue Eye Soluções em Tecnologia ("Partner") is authorized to distribute and resell CyberArk's products and services in Brazil.

Any and all CyberArk products provided by Partner are furnished based on CyberArk's standard license and support terms.

If you have any questions or need more information regarding this relationship, please do not hesitate to contact the undersigned.

Yours sincerely,

By DocuSigned by: F43AD5D5E928429...

Name Alvaro Fehr

Title Channel Director LATAM

Date June 25, 2025

ITEM	ID-SIGA	Descrição	Unidade	Quantidade	Marca/Modelo Ofertado
1	188644	Subscrição de Licença para Proteção Local e Elevação de Privilégio em servidores, com suporte técnico, por de 12 (doze) meses	UN	5,997	**Marca:** Cyberark **Modelo:** Cyberark Endpoint Privilege Management for servers
2	189074	Subscrição de Licença para Proteção Local e Elevação de Privilégio em desktops, com suporte técnico, por 12 (doze) meses	UN	13,910	**Marca:** Cyberark **Modelo:** Cyberark Endpoint Privilege Management for desktop
3	189075	Subscrição de Solução de Autenticação Multifator Adaptativa, com suporte técnico, por 12 (doze) meses	UN	13,978	**Marca:** Cyberark **Modelo:** Cyberark MFA Adaptativo
4	189076	Subscrição de Solução de Logon Único Adaptativo para Identidades dos Colaboradores, com suporte técnico, por 12 (doze) meses	UN	13,948	**Marca:** Cyberark **Modelo:** Cyberark Identity SSO

Item	Atende?	Documentação	Observações
1. ESPECIFICAÇÕES TÉCNICAS	Sim	N/A	
1.1. Proteção local e elevação de privilégios em servidores (item 1):	Sim	N/A	
1.1.1. A solução deverá garantir a segurança para identidades e acessos para servidores com sistemas operacionais Microsoft Windows e Linux.	Sim	https://docs.cyberark.com/EPM/Latest/en/Cont	Install the EPM agent
1.1.2. Requisitos mínimos aplicados a Servidores Windows:	Sim	N/A	
1.1.2.1. Prover as funcionalidades através de agentes instalados no sistema operacional e permitir a proteção e controle dos privilégios;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Install the EPM agent
1.1.2.2. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino;	Sim	https://docs.cyberark.com/epm-onprem/10.10/	Privileged Commands
1.1.2.3. Oferecer opções de execução sem aviso: de aplicações com privilégios em modo explícito e transparente, monitorada de aplicações em modo explícito e transparente, com restrições de aplicações em modo explícito e transparente;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	View existing policies
1.1.2.4. Exibir a reputação do arquivo executado advinda de, pelo menos, 1 (uma) fonte externa;	Sim	https://docs.cyberark.com/epm/latest/en/content/epm/server%20user%20guide/virus-total-integration.htm https://docs.cyberark.com/epm/latest/en/content/epm/server%20user%20guide/assess-threats.htm?Highlight=assess%20threats	Assess threats
1.1.2.5. Disponibilizar a opção de encaminhamento de arquivo suspeito para análise de malware em soluções de mercado;	Sim		
1.1.2.6. Suportar, no mínimo, os seguintes sistemas operacionais: Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022;	Sim	https://docs.cyberark.com/EPM/Latest/en/Cont	System requirements for EPM agents on Windows
1.1.2.7. Implementar regras de controle de aplicações permitidas e bloqueadas para execução fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Implement application control
1.1.2.8. Implementar regras de controle do nível de privilégio utilizado na execução das aplicações permitidas fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Implement application control

1.1.2.9. Implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Implement Privilege Management
1.1.2.10. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Overview
1.1.2.11. Permitir a criação de políticas reutilizáveis, contendo, no mínimo, os seguintes tipos de aplicações ou tipos de arquivos: executáveis, scripts, aplicações nativas Windows, bibliotecas dinâmicas (DLL), instaladores, controles ActiveX, objetos COM;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Windows parameters
1.1.2.12. Permitir a verificação do hash do arquivo, dos parâmetros permitidos e da assinatura de fabricante, para objetos reutilizáveis da solução;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Add application definitions
1.1.2.13. Suportar ao nome exato da aplicação / arquivo / script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Windows policies
1.1.2.14. Utilizar eventos reportados na interface da solução para criação de novas políticas ou incluí- los em políticas existentes;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Add applications to a police
1.1.2.15. Permitir agrupar aplicações com base em suas características, para facilitar a inserção de novas aplicações aos grupos ou políticas de segurança de aplicações já criadas;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Page features
1.1.2.16. Impedir a desativação das funcionalidades instaladas no sistema operacional alvo sem autorização e/ou registro da atividade por meio da console de gerência;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Protect agents
1.1.2.17. Disponibilizar o registro das execuções e atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido;	Sim	https://docs.cyberark.com/EPM-onprem/Latest/	Assess threats
1.1.2.18. Monitorar e exibir acessos e atividades realizadas na própria solução;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Types of reports
1.1.2.19. Permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras, individualmente ou em grupos;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Overview
1.1.2.20. Realizar varreduras utilizando as funcionalidades instaladas no sistema operacional alvo para catalogar arquivos existentes;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Scan applications
1.1.2.21. Possibilitar ao usuário final a solicitação de liberação de atividades específicas fazendo uso das funcionalidades instaladas no sistema operacional alvo;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Create an authorization code
1.1.2.22. Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Create a JIT policy

1.1.2.23. Implementar as regras de controle de acordo com características do usuário final, incluindo nome de usuário, grupos a que o usuário pertence e endereço IP;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Application policy guidelines
1.1.2.24. Oferecer monitoramento ou detecção quanto a tentativas de roubo de credenciais;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Protect against credential thef
1.1.2.25. Caso o dispositivo não possa estar conectado de forma permanente aos monitores/gravadores de acessos da solução e repositório seguro de credenciais, deve, de forma autônoma e off-line, gerenciar as senhas das credenciais locais, aplicando políticas de randomização e sincronização das senhas definidas na central da solução;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Create or customize a credentials rotation policy
1.1.2.26. Possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Create a policy
1.1.2.27. Permitir criar uma whitelist para execução de aplicativos confiáveis, onde qualquer outra aplicação fora desta lista automaticamente seja bloqueada;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Application definitions
1.1.2.28. Possuir uma integração com Windows UAC, e conter relatórios do uso de prompts aos usuários feitos pelo UAC;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Monitor user account control
1.1.2.29. Suportar a guarda de políticas de hosts que não fazem parte do Active Directory;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Customize policy targets
1.1.2.30. Possuir cache de políticas aplicadas no endpoint, permitindo a segurança dos endpoints, ainda que ele não esteja conectado à rede corporativa;	Sim	https://docs.cyberark.com/EPM/Latest/en/Cont	Policy enforcement protection
1.1.2.31. Permitir que mensagens customizadas sejam apresentadas antes que uma aplicação seja executada ou bloqueada;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Configure endpoint notifications
1.1.2.32. Deve suportar adição múltiplas mensagens, estas mensagens devem possibilitar edição e suportar múltiplas linguagens;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Create new notifications
1.1.2.33. Deve possuir capacidade de gerar relatórios de aplicações e eventos de usuários inclusos na solução;	Sim	https://docs.cyberark.com/pam-self-hosted/Late	Report types
1.1.2.34. Realizar varredura e inventário de aplicações instaladas no sistema operacional.	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Configure scanning
1.1.3. Requisitos mínimos aplicados Servidores Linux:	N/A		
1.1.3.1. Prover as funcionalidades através de agentes instalados no sistema operacional e permitir a proteção e controle dos privilégios;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Install the EPM agent
1.1.3.2. Garantir o controle 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	https://docs.cyberark.com/pam-self-hosted/Late	Privileged Commands
1.1.3.3. Suportar, no mínimo, os seguintes sistemas operacionais: Debian, Redhat Linux 7.x (64- bit), Redhat Linux 8.x (64-bit);	Sim	https://docs.cyberark.com/pam-self-hosted/late	Supported platforms

1.1.3.4. Disponibilizar, como conjunto mínimo de atividades controladas no ativo de destino, as seguintes operações: criação e exclusão de arquivos e diretórios, mudança de nome de arquivos e diretórios, abertura de arquivos para escrita, comandos chown e chmod e ligações entre arquivos;	Sim	https://docs.cyberark.com/pam-self-hosted/Late	Privileged Commands - PVWA
1.1.3.5. Implementar restrições, em uma plataforma, de maneira global ou em uma conta de usuário ou grupo de maneira granular;	Sim	https://docs.cyberark.com/pam-self-hosted/Late	Restrictions
1.1.3.6. Realizar o controle mediante interceptação do comando antes que ele seja executado;	Sim	https://docs.cyberark.com/pam-self-hosted/Late	Architecture
1.1.3.7. Permitir a liberação de comandos privilegiados a usuários comuns;	Sim		
1.1.3.8. Permitir que os comandos executados em sistemas monitorados sejam gravados em modo texto no repositório seguro digital;	Sim		
1.1.3.9. Permitir que sejam atribuídas permissões para usuários e grupos, inclusive do Active Directory;	Sim		
1.1.3.10. Permitir o agrupamento de comandos, bem como a utilização de coringas como (*), para uma definição ampla de parâmetros;	Sim		
1.1.3.11. A solução deverá possuir funcionalidade que permita definir variáveis de ambiente no momento da execução de um comando, independente da definição realizada pelo usuário ou seu perfil. Sendo exigido no mínimo as seguintes variáveis: PATH, ENV, BASH_ENV, GLOBIGNORE, SHELLOPTS;	Sim	https://docs.cyberark.com/pam-self-hosted/Late	Privilege command restrictions
1.1.3.12. Possibilitar o uso da máscara de usuário na execução dos comandos (valores entre 0000 e 0777);	Sim	https://docs.cyberark.com/pam-self-hosted/Late	SetUser Mask Override
1.1.3.13. Impedir a utilização da técnica de ShellEscape, em que um programa autorizado e executado com privilégios permita a execução de outros programas e consequentemente escape dos controles definidos;	Sim	https://docs.cyberark.com/pam-self-hosted/Late	Prevent Shell Escape
1.1.3.14. Disponibilizar a funcionalidade de restrição de Shell, que impossibilite que scripts e shells de sistema executem comandos não permitidos pelas regras definidas na solução;	Sim	https://docs.cyberark.com/pam-self-hosted/Late	Reset Environment Variables
1.1.3.15. Oferecer a capacidade de verificação da identidade da pessoa que executa comandos localmente no dispositivo alvo através de autenticação via usuário da ferramenta, LDAP ou RADIUS;	Sim	https://docs.cyberark.com/pam-self-hosted/Late	CyberArk Pluggable Authentication Module (PAM)
1.1.3.16. Monitorar e exibir acessos e atividades realizadas no próprio sistema;	Sim	https://docs.cyberark.com/pam-self-hosted/Late	What detections does PTA report?
1.1.3.17. Possibilitar mapear e coletar atividades regulares de usuários através do modo observação, agregando e exportando os resultados para um perfil;	Sim	https://docs.cyberark.com/epm/latest/en/conte	Default policies
1.1.3.18. Prover um controle de comandos completo, com a possibilidade de criar uma lista de comandos permitidos ou bloqueados (whitelisting/blacklisting), a serem alterados (criação de alias) ou prevenir que comandos sejam executados ou permitir trabalhar em Shell modificado/controlado;	Sim	https://docs.cyberark.com/pam-self-hosted/Late	Overview
1.1.3.19. 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	https://docs.cyberark.com/pam-self-hosted/Late	Privileged Commands - PVWA
1.2. Proteção local e elevação de privilégios em desktops (item 2)	N/A		
1.2.1. Prover as funcionalidades através de agentes instalados no sistema operacional e permitir a proteção e controle dos privilégios;	Sim	https://docs.cyberark.com/pam-self-hosted/Late	Privileged Commands

1.2.2. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino;	Sim	https://docs.cyberark.com/pam-self-hosted/Late	Privileged Commands
1.2.3. Realizar varredura e inventário de aplicações instaladas na estação de trabalho;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Scan applications
1.2.4. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente na estação de trabalho de destino (sem ser através do Repositório Seguro), fazendo uso das funcionalidades instaladas no sistema operacional;	Sim	https://docs.cyberark.com/epm/latest/en/conte	
1.2.5. Oferecer opção de execução de aplicações com privilégios em modo explícito e transparente (sem avisos);	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Policy actions
1.2.6. Oferecer opção de execução monitorada de aplicações em modo explícito e transparente (sem avisos);	Sim		
1.2.7. Oferecer opção de execução com restrições de aplicações em modo explícito e transparente (sem avisos);	Sim		
1.2.8. Exibir a reputação do arquivo executado advinda de, pelo menos, 1 (uma) fonte externa;	Sim	https://docs.cyberark.com/epm/25.5.0/en/conte	Assess threats
1.2.9. Disponibilizar a opção de encaminhamento de arquivo suspeito para análise de malware em soluções de mercado;	Sim		
1.2.10. Suportar pelo menos as seguintes versões de estações de trabalho: Windows 10 x32 & x64, Windows 11 x64;	Sim	https://docs.cyberark.com/EPM/Latest/en/Cont	System requirements for EPM agents on Windows
1.2.11. Implementar regras de controle de aplicações permitidas e bloqueadas para execução fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via Repositório Seguro ou diretamente no ativo;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Policy actions
1.2.12. Implementar regras de controle do nível de privilégio utilizado na execução das aplicações permitidas fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via mecanismo de Monitoramento Comportamental e Repositório Seguro ou diretamente no ativo;	Sim		
1.2.13. Implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Supported application definitions

1.2.14. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Customize and activate this policy
1.2.15. Permitir a criação de objetos reutilizáveis que possam conter no mínimo os seguintes tipos: arquivos executáveis, scripts, aplicações nativas Windows, bibliotecas dinâmicas (DLL), instaladores, controles ActiveX e objetos COM;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Definition properties
1.2.16. Implementar a verificação de hash do arquivo, dos parâmetros permitidos e da assinatura de fabricante, para objetos reutilizáveis da solução;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Windows parameters: Checksum
1.2.17. Implementar o suporte ao nome exato da aplicação/arquivo/script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Windows parameters: Interpreter
1.2.18. Utilizar eventos reportados na interface da ferramenta para novas políticas ou incluí-los em políticas existentes;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Add applications to a policy
1.2.19. Permitir agrupamento de características e aplicações para fácil seleção e inclusão em políticas de segurança;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	View aggregated event details
1.2.20. Impedir a desativação das funcionalidades instaladas no sistema operacional alvo sem autorização e/ou registro da atividade por meio da interface de gerência;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Extended protection
1.2.21. Disponibilizar modo de observação, em que não há bloqueios, mas há o registro das execuções e atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	View aggregated event details
1.2.22. Monitorar e exibir acessos e atividades realizadas na própria solução.	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Types of reports
1.3. Autenticação multi-fator adaptativa (item 3)	Sim	N/A	
1.3.1. A solução deverá ser capaz de atender minimamente os seguintes casos de uso para requisitar um e mais fatores de autenticação:	Sim	N/A	
I - Multi Fator de autenticação para soluções de VPN via RADIUS ou SAML.	Sim	https://docs.cyberark.com/identity/latest/en/co	
II - Qualquer dispositivo ou sistema operacional que suporte RADIUS.	Sim	https://docs.cyberark.com/identity/latest/en/co	
III - Plugin para ADFS (IDP, Identity Provider), Active Directory Federation Services.	Sim	https://docs.cyberark.com/identity/latest/en/co	

IV - Sob demanda utilizando o protocolo Oauth e REST APIs.	Sim	https://docs.cyberark.com/identity/latest/en/co	
V - Para realizar o autosserviço de reset de senha ou desbloqueio de usuário.	Sim	https://docs.cyberark.com/identity/latest/en/co	
1.3.2. A solução deverá ser capaz de oferecer minimamente os seguintes métodos para múltiplo fator de autenticação:	Sim	N/A	
I - Usuário e senha dos diretórios suportados na solução.	Sim	https://docs.cyberark.com/identity/latest/en/co	
II - Através de aplicativo para dispositivos móveis do tipo IOS e Android, oferecendo suporte para:	Sim	N/A	
a) Biometria do tipo FaceID.	Sim	https://docs.cyberark.com/identity/latest/en/co	
b) Biometria através do leitor de digital.	Sim	https://docs.cyberark.com/identity/latest/en/co	
c) Smartphone push (Notificação para aprovar ou recusar uma autenticação).	Sim	https://docs.cyberark.com/identity/latest/en/co	
d) Geolocalização a banco de dados de IPs.	Sim	https://docs.cyberark.com/identity/latest/en/co	
e) Suporte a tokens OATH OTP.	Sim	https://docs.cyberark.com/identity/latest/en/co	
f) Autenticação na tela de login via QRcode sem a necessidade de digitar usuário e senha, com opção de forçar a biometria no dispositivo móvel.	Sim	https://docs.cyberark.com/identity/latest/en/co	
g) Ligação telefônica requisitando um PIN previamente configurado.	Sim	https://docs.cyberark.com/identity/latest/en/co	
h) Mensagem de texto via SMS oferecendo o código para entrada manual e também uma URL única presente na mensagem de texto que ofereça a opção de aprovar ou recusar a autenticação sem a necessidade de digitar o código manualmente.	Sim	https://docs.cyberark.com/identity/latest/en/co	
i) Confirmação de código via email.	Sim	https://docs.cyberark.com/identity/latest/en/co	
j) Clientes do tipo OATH OTP (exemplo, Google Authenticator).	Sim	https://docs.cyberark.com/identity/latest/en/co	

k) Autenticadores que suportem FIDO2 / U2F, minimamente suportando: Windows Hello, Yubikey, Google Titan Key, MacOS TouchID e Perguntas e respostas previamente configuradas.	Sim	https://docs.cyberark.com/identity/latest/en/co	
III - Permitir que os usuários realizem o autosserviço de reset de senha e desbloqueio de usuário utilizando os métodos de múltiplo fator de autenticação citados para verificação positiva através do portal web da solução.	Sim	https://docs.cyberark.com/identity/latest/en/co	
IV - Permitir que os usuários realizem o autosserviço de reset de senha e desbloqueio de usuário utilizando os métodos de múltiplo fator de autenticação citados para verificação positiva através de REST APIs oferecidas pela solução.	Sim		
V - É desejável que a solução possibilite integrações e customizações através de SDK (Software Development Kits) para aplicações mobile. Estes SDKs não devem ter um custo adicional;	Sim	https://docs.cyberark.com/identity/latest/en/co	
VI - Para cada caso de uso ou conjunto de casos de uso de múltiplo fator de autenticação citados, a solução de ser capaz de identificar os atributos de contexto de cada autenticação para disponibilizar os melhores métodos definidos para a autenticação, suportando minimamente:	Sim	N/A	
a) Endereçamento IP.	Sim	https://docs.cyberark.com/identity/latest/en/co	
b) Dia da Semana.	Sim		
c) Datas específicas.	Sim		
d) Janelas de tempo entre duas datas.	Sim		
e) Janelas de tempo entre horários (exemplo, horário comercial).	Sim		
f) Tipo do Sistema Operacional.	Sim		
g) Tipo do Browser.	Sim		
h) Perfis configurados na solução.	Sim		
i) País que está sendo realizado o acesso.	Sim		
j) Se é um dispositvo gerenciado.	Sim		
k) Autenticação via certificado.	Sim		
l) Nível de Risco da autenticação medido por um motor de análise de comportamento dos usuários.	Sim		
VII - A solução deve ter a capacidade de verificar antes de realizar um login em uma aplicação se o endpoint gerenciado está em conformidade com a solução de gerenciamento de endpoint (Unified Endpoint Management UEM), devendo suportar minimamente:	Sim	N/A	
a) Microsoft Intune	Sim	https://docs.cyberark.com/identity/latest/en/co	
b) VmWare Workspace Obe	Sim		
c) JAMF	Sim		
VIII - A solução deve ter capacidade de detectar casos de uso e perfis de autenticação já validados pelos usuários e não requisitar mais os mesmos durante um período de tempo configurado pelo administrador da solução, evitando desta forma repetidas validações em um curto espaço de tempo.	Sim	https://docs.cyberark.com/identity/latest/en/co	
IX - O conjunto de fatores de autenticação disponibilizados devem ser baseados durante o acesso através de regras especificadas no item anterior e segregados por:	Sim	N/A	

a) Conjunto de aplicações.	Sim	https://docs.cyberark.com/identity/latest/en/co	
b) Um única aplicação.	Sim	https://docs.cyberark.com/identity/latest/en/co	
c) Regras para o autosserviço de reset de senha e desbloqueio de usuário.	Sim	https://docs.cyberark.com/identity/latest/en/co	
d) Portal do Administrador.	Sim	https://docs.cyberark.com/identity/latest/en/co	
e) Portal do Usuário.	Sim	https://docs.cyberark.com/identity/latest/en/co	
X - A solução deve prover um portal WEB para o usuário final;	Sim		
XI - Permitir o usuário realizar o auto-registro de seus fatores de autenticação, tais como, perguntas e respostas, FIDO2 tokens, OATH OTP, definir PIN para chamada telefônica, TouchID, FaceID, Windows Hello, dentre outros.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XII - Permitir o usuário redirecionar autenticação multi-fator para outros usuários (desde que permitido).	Sim	https://docs.cyberark.com/identity/latest/en/co	
XIII - Permitir os usuários gerenciarem seus dispositivos registrados, para Smartphones Android, IOS	Sim	https://docs.cyberark.com/identity/latest/en/co	
XIV - Permitir aos usuários a capacidade de gestão para realizar o auto-registro de novos dispositivos móveis.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XV - Configurar OATH OTP para autenticação multi-fator nos sistemas operacionais Windows e MacOS (telas de login e bloqueio) quando os mesmo estão desconectados da internet com a finalidade de prover MFA mesmo quando sem internet para o sistema operacional.	Sim	https://docs.cyberark.com/identity-administrati	
XVI - A solução deve prover um aplicativo móvel para Android e IOS;	Sim		
XVII - Permitir configurar OATH OTP adicionais provenientes de outras soluções.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XVIII - Deve verificar dispositivos registrados (dispositivos móveis e sistemas operacionais).	Sim	https://docs.cyberark.com/identity/latest/en/co	
XIX - Deve ter integração nativa com FaceID, TouchID, leitor biométrico dos dispositivos móveis alavancando os mesmos para autentição biométrica durante login nas aplicações.	Sim	https://docs.cyberark.com/remote-access-stand	
XX - Deve reportar coodernadas GPS para os sistemas que utilizam geolocalização.	Sim	Configure device location reporting and tracking | CyberArk Docs	

XXI - Deve detectar ROOT em dispositivos Android e Jailbreak em dipositivos IOS com a finalidade de detectar atividades maliciosas e como consequência o aplicativo é desabilitado para uso	Sim	https://docs.cyberark.com/identity/latest/en/co	
XXII - O aplicativo deve suportar autenticação do tipo push, onde o usuário tem a escolha de aceitar ou recusar o desafio, esta notificação de conter minimamente:	Sim	N/A	
a) Data e Hora.	Sim	https://docs.cyberark.com/identity/latest/en/co	
b) Cidade / Geolocalização do acesso	Sim	https://docs.cyberark.com/identity/latest/en/co	
c) Aplicação sendo acessada.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XXIII - A solução deve possuir a capacidade de realizar o login sem a utilização da senha (passwordless) realizando o scan de QR code gerado na tela de login do portal de aplicação através do aplicativo móvel do fabricante, sem a necessidade inclusive de digitar o usuário a ser logado na aplicação. Deve adicionalmente ter a opção de forçar a utilização de biometria oferecida pelo smartphone / telefone celular.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XXIV - A solução deve possuir um aplicativo para Windows e MacOs com suporte a multifator de autenticação do tipo OTP (one time password) do próprio fabricante da solução de multifator. Este aplicativo dará suporte para casos onde não será possível o uso de um telefone celular / smartphone.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XXV - Permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras, individualmente ou em grupos;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Overview
a) Deve realizar varreduras fazendo uso das funcionalidades instaladas no sistema operacional alvo para catalogar arquivos existentes nas máquinas e uni-los ao inventário populado mediante detecção durante a execução;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Configure scanning
b) Deve verificar a reputação dos arquivos executados e detectados pelas funcionalidades instaladas no sistema operacional alvo ou mecanismos de controle de ameaças (VirusTotal.com ou similares);	Sim	https://docs.cyberark.com/epm/latest/en/content/epm/server%20user%20guide/virus-total-integration.htm https://docs.cyberark.com/epm/latest/en/content/epm/server%20user%20guide/assess-threats.htm?Highlight=assess%20threats	Assess threats
c) Permitir a execução automática de tipos desconhecidos de arquivo, de acordo com sua origem, mesmo possuindo restrições;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Policy actions
XXVI - Possibilitar ao usuário final a solicitação de liberação de atividades específicas fazendo uso das funcionalidades instaladas no sistema operacional;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Request temporary access to applications
XXVII -Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Enable authorization codes

XXVIII - Implementar as regras de controle de acordo com características do usuário final, incluindo nome de usuário, grupos a que o usuário pertence e endereço IP;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Customize policy targets
XXIX - Permitir o envio de arquivos suspeitos, executados sob sua supervisão, para soluções de análise de ameaça do tipo Sandbox.	Sim	https://docs.cyberark.com/EPM/Latest/en/Cont	Configure integration settings
XXX - Possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados.	Sim	https://docs.cyberark.com/epm/latest/en/Conte	Create a policy
XXXI - Permitir a salvaguarda das contas privilegiadas em um único repositório seguro.	Sim	https://docs.cyberark.com/pam-self-hosted/late	
XXXII -A solução deve fornecer proteção de grupos de privilégios, o que significa que os usuários não podem adulterar ou modificar grupos privilegiados locais, como o grupo Administradores ou Power Users;	Sim	https://docs.cyberark.com/epm/latest/en/conte	
XXXIII - Solução deve automaticamente permitir os aplicativos de lista branca implantados por ferramentas de implantação de software por administradores confiáveis, incluindo o SCCM (Microsoft System Center Configuration Manager)	Sim	https://docs.cyberark.com/epm-onprem/10.10/	
XXXIV - a Solução deve permitir criar uma lista de aplicativos permitidos (allow list), onde seja possível configurar todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista seja bloqueada automaticamente.	Sim	https://docs.cyberark.com/epm/latest/en/content/epm/server%20user%20guide/privmgmnt-blockunhandledapps-newui.htm https://docs.cyberark.com/epm/latest/en/content/epm/server%20user%20guide/predefinedpolicies-newui.htm https://docs.cyberark.com/epm/latest/en/content/intro/implement%20privilege%20management.htm	
XXXV -Permitir criar uma lista branca (whitelist) de aplicativos, onde é configurado todos os aplicativos que podem ser executados, onde qualquer outra aplicação fora desta lista, seja automaticamente seja bloqueada;	Sim	https://docs.cyberark.com/epm/latest/en/Conte	View application groups
XXXVI - a Solução dever ser baseada em algoritmos de aprendizado de máquina (Machine Learning) não supervisionados, ou seja, os modelos estatísticos com os casos de uso já prontos e calibrados para cálculo de risco.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XXXVII - A solução deve medir o risco da autenticação verificando o comportamento histórico da identidade através do conjunto dos seguintes atributos:	**Sim**	N/A	
a) Geo Velocidade, medindo velocidade de deslocamento do login, comparando a localização do último login com a atual, evitando "viagens impossíveis", e traçando o comportamento do usuário neste quesito, por exemplo, pessoas que viajam muito podem ter uma pontuação de risco baixa mesmo que sua Geo Velocidade seja maior que pessoas que não viajam.	Sim	https://www.cyberark.com/products/user-behav	
b) Geo Localização: medindo o risco da autenticação verificando sua localização geográfica do acesso atual em comparação com o seu comportamento usual.	Sim	https://www.cyberark.com/products/user-behav	
c) Dia da Semana: medindo o risco da autenticação verificando o dia da semana do acesso atual em comparação com seu comportamento usual.	Sim	https://www.cyberark.com/products/user-behav	
d) Horário do Acesso: mede o risco da autenticação verificando o horário do acesso atual em comparação com seu comportamento usual.	Sim	https://www.cyberark.com/products/user-behav	

e) Sistema Operacional: mede o risco da autenticação verificando o Sistema Operacional do acesso atual em comparação com seu comportamento usual.	Sim	https://docs.cyberark.com/identity/latest/en/co	
f) Falhas de login consecutivas, mede o risco da autenticação verificando as falhas de login consecutivas do acesso atual em comparação com seu comportamento usual	Sim	https://docs.cyberark.com/identity/latest/en/co	
g) O cálculo do risco pelo motor de aprendizado de máquina não utilize somente um atributo fora da normalidade reconhecida anteriormente pelo mesmo, mas sim em uma única autenticação calcule o risco baseado em todos os atributos citados acima e suas anormalidades em uma única autenticação. Exemplo, uma identidade tem por costume realizar sua autenticação as 9,10 e 11 da manhã, nas aplicações A e B, nas segundas-feiras e quintas-feiras, utilizando um dispositivo Android, das cidades de Brasília e São Paulo. Em futuro login acababa realizando a autenticação as 14 horas (fora do seu horário regular), na aplicação A, em um sábado (não é um dia da semana usual para esta identidade), de um dipositivo IOS (também não usual), da cidade de Brasília. O motor de aprendizado de máquina deve ter a capacidade de reconhecer estes três desvios de comportamento e retornar um risco calculado (alto, médio, baixo ou sem risco) referente a mesma.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XXXVIII - a Solução deverá prover múltiplo fator de autenticação para casos de uso com capacidade de interpretação de risco adaptativo baseados em algotimos de aprendizado de máquina e reconhecimento de comportamentos temporais para cada identidade (dias da semana e horários), o mesmo calculado antes da autenticação para tomada de ações antes da materialização da autenticação.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XXXIX - Deve prover a personalização das faixas de pontuação (0 a 100) para os administradores da solução para, no mínimo, as categorias:	Sim	N/A	
a) Sem risco	Sim	https://docs.cyberark.com/identity/latest/en/co	
b) Risco Baixo	Sim		
c) Risco Médio	Sim		
d) Risco Alto	Sim		
XL - Deve prover para os administradores da solução a personalização da influência na medição do risco para cada atributo citado neste item. Por exemplo, para a CONTRATANTE a geo velocidade pode ser um fator que não possui relevância, desta forma deve ser possível configurar a influência deste risco como baixa na modelagem de risco da plataforma;	Sim	https://docs.cyberark.com/identity/latest/en/co	
XLI - O risco calculado durante a autenticação pelo motor de análise do comportamento dos usuários deve ser compartilhado com funções de Múltiplo Fator de autenticação que realizam o login para os casos de uso citados neste documento e utilizar como contexto para:	**Sim**	N/A	

a) Requisitar múltiplos fatores de autenticação de forma dinâmica.	Sim	https://docs.cyberark.com/identity/latest/en/co	
b) Permitir o login sem o uso de múltiplos fatores.	Sim	https://docs.cyberark.com/identity/latest/en/co	
c) Negar a autenticação.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XLII - Deve prover para os administradores da solução a capacidade de explorar os dados históricos através de dashboards, filtros e gráficos configuráveis sendo possível verificar os alertas e os fatores que os influenciaram, além da exploração dos eventos capturados e seus atributos.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XLIII - Deve prover gráficos de linha do tempo, donuts, mapas com geolocalização dos eventos, gráfico de barras, tabelas analíticas, e mapas de relacionamento, sendo suas dimensões e categorias personalizáveis	Sim	https://docs.cyberark.com/identity/latest/en/co	
XLIV - Deve ser capaz de exportar os dados dos alertas, riscos calculados, eventos para, no mínimo, CSV, adicionalmente gravar as visualizações na solução para consultas posteriores.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XLV - Deve possuir integração com fontes de inteligência cibernética de terceiros reconhecidas no mercado, como, por exemplo, Palo Alto Cloud.	Sim	https://docs.cyberark.com/EPM-onprem/Latest/	
XLVI - Deve possuir interface para envio de alertas de forma automatizada, suportando, no mínimo E-mail com conteúdo do alerta e Webhooks (ex: envio de mensagem para um canal do Microsoft Teams ou Slack.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XLVII - Possuir dashboards pré-configurados com informações e gráficos com as seguintes caracteríticas:	Sim	N/A	
a) Utilização do Motor de Análise do Comportamento dos Usuários.	Sim	https://docs.cyberark.com/identity/latest/en/content/coreservices/reports/dashboardsview.htm?tocpath=Administrator%7C_____14	
b) Comportamento dos usuários na utilização das aplicações.	Sim		
c) Visão sobre a segurança das aplicações.	Sim		
d) Mapa com a geolocalização das autenticações.	Sim		
e) Visão sobre o comportamento dos Endpoints (Mobile e Computadores).	Sim		
f) Visão sobre o comportamento das Identidades.	Sim		

XLVIII - A solução deve permitir a configuração de dashboards personalizados.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XLIX - Deve permitir o compartilhamento dos dashboards com outros usuários.	Sim	https://docs.cyberark.com/identity/latest/en/co	
1.4. Logon único adaptativo para identidades dos colaboradores (item 4)	Sim		N/A
I - A solução deve prover um catálogo de aplicações Web com modelos de configuração de Single Sign-On (SSO) abrangendo as aplicações mais conhecidas de mercado, com a finalidade de facilitar a configuração destas integrações.	Sim	https://docs.cyberark.com/identity/latest/en/Co	
II - A solução deve permitir a configuração do SSO para aplicações Web minimamente através dos seguintes protocolos e métodos:	Sim		N/A
a) SAML 2.0	Sim	https://docs.cyberark.com/identity/latest/en/co	
b) Oauth 2.0 modo client	Sim		
c) WS-Federation	Sim		
d) OpenID connect	Sim		
e) NTLM	Sim		
f) Oauth 2.0 modo server	Sim		
g) HTTP Basic	Sim		
III - Suportar SSO via IWA (Integrated Windows Authentication) o qual reutiliza o login de rede para autenticação nas aplicações web, sem a necessidade de digitar usuário e senha novamente.	Sim	https://docs.cyberark.com/identity/latest/en/co	
IV - Oferecer suporte para a personalização das repostas SAML, como por exemplo, mapear atributos dos diretórios para atributos SAML, ter a capacidade de incluir lógicas complexas para manipulação das repostas SAML e possibilitar a visualização da reposta SAML configurada antes de sua implantação.	Sim	https://docs.cyberark.com/identity/latest/en/co	
V - A solução deve prover um portal WEB para o usuário final com as seguintes características:	Sim		N/A
a) Depois de efetuado o login apresentar as aplicações WEB disponíveis para realizar o SSO, através de um conjunto de ícones onde cada um representa uma aplicação que o usuário tem o direito de efetuar o SSO;	Sim	https://docs.cyberark.com/identity/latest/en/co	
b) Realizar mudanças em atributos da identidade, tais como, telefone celular, email e foto.	Sim		
c) Verificar as atividades de sua identidade através de dashboard com as seguintes informações:	Sim		N/A
A) Total de logons.	Sim	https://docs.cyberark.com/identity/latest/en/co	
B) Total de falhas de logon.	Sim		
C) Geolocalização dos seus logons.	Sim		
D) Verificar a Geolocalização atual de seus dispositivos registrados.	Sim		
E) Utilização das aplicações.	Sim		
F) Histórico de eventos importantes, tais como, nova aplicação adicionada em seu portal de SSO, falhas delogon, dentre outros.	Sim		

VI - Deve possuir serviço de diretório para armazenar identidades na solução, sem a dependência da sincronização com outros serviços de diretório on-premisses ou na nuvem de terceiros.	Sim	https://docs.cyberark.com/identity/latest/en/co	
VII - O serviço de diretório da solução deve ser auto-escalável para suportar um grande número de identidades e multiplas autenticações simultâneas.	Sim	https://www.cyberark.com/products/directory-s	
VIII - Deve ter a capacidade de forçar a complexidade das senhas, minimamente para os seguintes requisitos:	Sim	N/A	
a) Tamanho mínimo.	Sim	https://docs.cyberark.com/identity/latest/en/co	
b) Tamanho máximo.	Sim		
c) Requerer mínimo de dígitos.	Sim		
d) Requerer letras maiúsculas e minúsculas.	Sim		
e) Requerer caracter especial (símbolo).	Sim		
f) Limitar caracteres consecutivos.	Sim		
g) Forçar expiração de senhas baseadas na idade das mesmas.	Sim		
h) Guardar histórico de senhas para evitar reutilização	Sim		
IX - Prover notificação para expiração das senhas por email.	Sim		
X - Capturar falhas de logon repetidas para bloqueio do usuário	Sim		
XI - A solução deve suportar adicionalmente a integração com serviços de diretório On-premisses e em nuvem, suportando minimamente:	Sim	N/A	
a) Microsoft Active Directory.	Sim	https://docs.cyberark.com/identity/latest/en/co	
b) Microsoft Azure AD	Sim		
c) Google Directory	Sim		
d) Diretórios LDAP	Sim		
XII - As integrações realizadas com diretório de terceiros não devem realizar sincronismo com estas bases, ou seja, carregar todo o diretório configurado para a nuvem, a solução deve atuar como um intermediário (“broker”) entre os serviços de diretório de terceiros e a solução.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XIII - A solução deve possuir integração com provedores de identidades sociais com a finalidade de delegar a autenticação para tais provedores e atender possíveis requisitos de negócio, suportando minimamente os seguintes provedores:	Sim	N/A	
a) Google.	Sim	https://docs.cyberark.com/identity/latest/en/co	
b) Facebook.	Sim		
c) LinkedIn.	Sim		
d) Microsoft.	Sim		
XIV - A solução deve ter a capacidade de configurar IDPs (Identity Providers) de parceiros de negócio da CONTRATANTE para dar acesso às identidades federadas em aplicações de negócio da CONTRATANTE sem a necessidade de criação de uma nova identidade na infraestrutura, por meio de federação realizada através do protocolo SAML.	Sim	https://docs.cyberark.com/identity/latest/en/co	

XV - A solução deve ter a capacidade de configurar um timeout por sessão e quantidade de sessões simultâneas, desta forma quando a sessão atingir tal tempo configurado de inatividade ou sessões simultâneas realizar o logout automático deste usuários nas aplicações conectadas.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XVI - O conector on premisses da solução que faz a comunicação do datacenter do cliente com a nuvem da solução SaaS deve ser único e sem a necessidade de instalação de componentes individuais para cada papel que o mesmo desempenhará, adicionalmente não deve depender de componentes de terceiros para ter alta disponibilidade e balanceamento de carga (exemplo, balanceadores de carga de terceiros). Em um único serviço ou agente on premisses deve englobar minimamente os seguintes componentes:	Sim	N/A	
a) Servidor RADIUS	Sim		
b) Cliente Radius	Sim		
c) Proxy reverso	Sim		
d) Integração com LDAP e Microsoft AD	Sim		
e) IWA, Integrated Windows Authentication	Sim	https://docs.cyberark.com/identity/latest/en/co	
XVII - A solução deve oferecer um componente/software para intermediar o SSO em aplicações Web sitiadas no datacenter da CONTRATANTE sem a necessidade de expor estas aplicações para a internet ou uso de VPN e deve suportar os mesmos métodos e protocolos do item anterior.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XVIII - A solução dever ser baseada em algoritmos de aprendizado de máquina (Machine Learning) não supervisionados, ou seja, os modelos estatísticos com os casos de uso já prontos e calibrados.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XIX - A solução deve medir o risco da autenticação verificando o comportamento histórico da identidade através do conjunto dos seguintes atributos:	Sim	N/A	
a) Geolocalização: medindo o risco da autenticação verificando sua localização geográfica do acesso atual em comparação com o seu comportamento usual.	Sim	https://www.cyberark.com/products/user-behav	
b) Dia da Semana: medindo o risco da autenticação verificando o dia da semana do acesso atual em comparação com seu comportamento usual.	Sim	https://www.cyberark.com/products/user-behav	
c) Horário do Acesso: mede o risco da autenticação verificando o horário do acesso atual em comparação com seu comportamento usual.	Sim	https://www.cyberark.com/products/user-behav	
d) Sistema Operacional: mede o risco da autenticação verificando o Sistema Operacional do acesso atual em comparação com seu comportamento usual	Sim	https://docs.cyberark.com/identity/latest/en/co	
e) Falhas de login consecutivas, mede o risco da autenticação verificando as falhas de login consecutivas do acesso atual em comparação com seu comportamento usual	Sim	https://docs.cyberark.com/identity/latest/en/co	

f) Deve prover a personalização das faixas de pontuação (0 a 100) para os administradores da solução para, no mínimo, as categorias:	Sim	N/A	
A) Sem risco	Sim		
B) Risco Baixo	Sim		
C) Risco Médio	Sim		
D) Risco Alto	Sim	https://docs.cyberark.com/identity/latest/en/co	
XX - O risco calculado durante a autenticação pelo motor de análise do comportamento dos usuários deve ser compartilhado com funções de Múltiplo Fator de autenticação e Single Sign-On que realizam o login para os casos de uso citados neste documento e utilizar como contexto para:	Sim	N/A	
a) Requisitar múltiplos fatores de autenticação de forma dinâmica.	Sim	https://docs.cyberark.com/identity/latest/en/co	
b) Permitir o login sem o uso de múltiplos fatores.	Sim	https://docs.cyberark.com/identity/latest/en/co	
c) Negar a autenticação.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XXI - Deve prover para os administradores da solução a capacidade de explorar os dados históricos através de dashboards, filtros e gráficos configuráveis sendo possível verificar os alertas e os fatores que os influenciaram, além da exploração dos eventos capturados e seus atributos.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XXII - Deve prover gráficos de linha do tempo, donuts, mapas com geolocalização dos eventos, gráfico de barras, tabelas analíticas, e mapas de relacionamento, sendo suas dimensões e categorias personalizáveis	Sim	https://docs.cyberark.com/identity/latest/en/co	
XXIII - Deve ser capaz de exportar os dados dos alertas, riscos calculados, eventos para, no mínimo, CSV, adicionalmente gravar as visualizações na solução para consultas posteriores.	Sim	https://docs.cyberark.com/identity/latest/en/co	

XXIV - Deve possuir integração com fontes de inteligência cibernética de terceiros reconhecidas no mercado.	Sim	https://docs.cyberark.com/epm-onprem/10.10/	
XXV - Deve possuir interface para envio de alertas de forma automatizada, suportando, no mínimo:	Sim		N/A
a) E-mail com conteúdo do alerta.	Sim	https://docs.cyberark.com/identity/latest/en/co	
b) Webhooks (ex: envio de mensagem para um canal do Microsoft Teams ou Slack.	Sim		
XXVI - Possuir dashboards pré-configurados com informações e gráficos com as seguintes características:	Sim		N/A
a) Utilização do modelo de Análise do Comportamento dos Usuários.	Sim	https://docs.cyberark.com/identity/latest/en/content/coreservices/reports/dashboardsview.htm?tocpath=Administrator%7C_____14	
b) Comportamento dos usuários na utilização das aplicações.	Sim		
c) Visão sobre a segurança das aplicações.	Sim		
d) Mapa com a geolocalização das autenticações.	Sim		
e) Visão sobre o comportamento dos Endpoints (Mobile e Computadores).	Sim		
f) Visão sobre o comportamento das Identidades.	Sim		
XXVII -A solução deve permitir a configuração de dashboards personalizados.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XXVIII - Deve permitir o compartilhamento dos dashboards com outros usuários.	Sim	https://docs.cyberark.com/identity/latest/en/co	
XXIX - A solução deve permitir que as aplicações acessadas através do portal Single Sign-on sejam monitoradas e indexadas em uma linha do tempo, registrando a navegação do usuário na página web.	Sim	https://docs.cyberark.com/sws/latest/en/conter	
XXX - Deve registrar cliques de janela e textos utilizados durante a navegação do usuário final na aplicação monitorada.	Sim	https://docs.cyberark.com/sws/latest/en/conter	
XXXI - Deve permitir ao administrador, acessos a screenshots da navegação do usuário final na página web da aplicação, que identificam visualmente o campo modificado em destaque e o momento exato da ação durante a navegação.	Sim	https://docs.cyberark.com/sws/latest/en/conter	
XXXII -Deve permitir ao administrador pesquisar por meio da seleção de aplicações gerenciadas no portal e campos indexados, como textos e campos acessados durante a navegação.	Sim	https://docs.cyberark.com/sws/latest/en/conter	
XXXIII - deve permitir o isolamento da sessão do browser para aplicações web monitoradas, não permitindo a função copiar e colar e qualquer tipo de download da sessão isolada, dessa forma evitando o vazamento de informações desta sessão web protegida.	Sim	https://docs.cyberark.com/sws/latest/en/conter	
XXXIV - deve permitir gravação da sessões em nuvem, a fim de não onerar espaço de armazenamento on premisses do órgão contratante.	Sim	https://docs.cyberark.com/sws/latest/en/conter	

XXXV -Deve permitir iniciar gravação, monitoramento contínuo e isolamento de sessão web por aplicação e perfil de acesso.	Sim	https://docs.cyberark.com/sws/latest/en/conter	
XXXVI - deve alertar o usuário final de maneira visual, antes de iniciar o processo de monitoramento e gravação da sessão.	Sim	https://docs.cyberark.com/sws/latest/en/conter	