



**MINISTÉRIO DA CULTURA**  
**COORDENAÇÃO DE INFRAESTRUTURA TECNOLÓGICA**

Edifício Parque Cidade Corporate, Torre B, 10º andar - Bairro Asa Sul, Brasília/DF, CEP 70308-200  
Telefone: - <http://www.cultura.gov.br>

**CADERNO DE ESPECIFICAÇÕES TÉCNICAS**

**ANEXO I**

*Obs.: caso haja divergências entre este documento e os demais que fazem parte do edital, deverá prevalecer o constante neste documento.*

**PROCESSO: 01400.013416/2023-42**

**DOCUMENTOS RELACIONADOS:**

Estudo Técnico Preliminar: 53/2024

Termo de Referência: (em elaboração)

**OBJETO:** Contratação de Subscrição para solução de segurança para Gestão de Identidade e Gestão de Acesso por doze (12) meses, garantia de suporte e atualização.

**QUADRO DE COMPOSIÇÃO - GRUPO E ITENS**

Grupo	Item	Descrição	Unidade	Qtd.
01	1	Subscrição para solução de segurança para identidades e acessos - Logon único adaptativo para identidades dos usuários.	Usuários	1800
	2	Subscrição para solução de segurança para identidades e acessos - Autenticação multi-fator adaptativa para identidades dos usuários.	Usuários	1800
	3	Subscrição para solução de segurança para identidades e acessos - Monitoramento comportamental e mitigação de riscos das identidades privilegiadas.	Usuários	200
	4	Subscrição para solução de Segurança para Armazenamento de Credenciais.	Usuários	3800
	5	Subscrição para solução de segurança para identidades e acessos - Proteção Local para Servidores Windows.	Servidor	70
	6	Subscrição para solução de segurança para identidades e acessos - Proteção Local para Servidores Linux/Unix.	Servidor	250
	7	Subscrição para solução de segurança para identidades e acessos - Proteção Local para Estações de Trabalho.	Estação de Trabalho	1800
	8	Subscrição para solução de segurança para identidades e acessos - Proteção para Aplicações Containerizadas.	Cluster	1
	9	Subscrição para solução de segurança para identidades e acessos - Proteção para Aplicações.	Aplicação	100
	10	Serviço de Instalação e Configuração das Soluções (por item / módulo)	Serviço	11
	11	Serviço de treinamento / capacitação (por item / módulo)	Turma	11
02	12	Serviço de acesso remoto confiança zero (ZTNA)	Usuários	800
	13	Serviço de acesso seguro interno/externo (SWG)	Usuários	3700
	14	Serviço de Instalação e Configuração das Soluções (por item / módulo)	Serviço	4
	15	Serviço de treinamento / capacitação (por item / módulo)	Turma	4

# 1. **CARACTERÍSTICAS GERAIS PARA OS ITENS 01, 02, 03, 04, 05, 06, 07, 08, 09, 12 E 13**

1.1. Os serviços de fornecimento de subscrição contempla a

disponibilização das licenças em um repositório do fabricante para total acesso do CONTRATANTE a quantidade de licenças contratadas, devendo a CONTRATADA tomar todas as providências necessárias junto ao fabricante para a liberação de acesso ao ambiente de monitoramento/repositório para o controle de licenças.

1.2. Caberá a CONTRATADA auxiliar a equipe indicada pela CONTRATANTE quanto aos procedimentos necessários para a instalação de ao menos 20% das licenças contratadas repassando o conhecimento para que as demais atividades rotineiras de instalação desinstalação e gestão dos licenças sejam realizadas pela equipe técnica do CONTRATANTE, os procedimentos de aceite definitivo somente poderão ser iniciados após a conclusão da instalação mínima de 20% das licenças contratadas.

1.3. Caberá a CONTRATADA garantir que todos os softwares tenham garantia de suporte e atualização durante os doze (12) meses, garantido a atualização e suporte técnico para a CONTRANTE junto ao fabricante das soluções contratadas ou mesmo por meio de atuação da equipe técnica da CONTRATADA.

## **2. ITEM 01 - SUBSCRIÇÃO PARA SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS - LOGON ÚNICO ADAPTATIVO PARA IDENTIDADES DOS USUÁRIOS**

2.1. 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.

2.2. A solução deve permitir a configuração do SSO para aplicações Web minimamente através dos seguintes protocolos e métodos:

a) SAML 2.0

b) Oauth 2.0 modo client

c) WS-Federation

d) OpenID connect

e) NTLM

f) Oauth 2.0 modo server

g) HTTP Basic

h) Extensão no Browser para capturar aplicações Web que utilizam formulário com usuário e senha e realizar o auto preenchimento do login e senha de forma automatizada. Estas informações devem ser guardadas de forma segura na solução para auto preenchimento nos futuros logins nestas aplicações.

2.3. A solução deve prover uma extensão de browser avançada somente para administradores da solução, com a finalidade de realizar o mapeamento dos campos dos fomulários (em geral login e senha) para que depois de mapeados os administrados possam incluir como uma aplicação Web para SSO no catálogo geral, permitindo o SSO de aplicações que não suportam protocolos mais modernos como SAML e Oauth.

2.4. 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.

2.5. 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.

2.6. A solução deve prover um portal WEB para o usuário final com as seguintes características:

- 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
- b) Realizar mudanças em atributos da identidade, tais como, telefone celular, email e foto.
- c) Verificar as atividades de sua identidade através de dashboard com as seguintes informações:
  - I - Total de logons.
  - II - Total de falhas de logon.
  - III - Geolocalização dos seus logons.
  - IV - Verificar a Geolocalização atual de seus dispositivos registrados.
  - V - Utilização das aplicações.
  - VI - Histórico de eventos importantes, tais como, nova aplicação adicionada em seu portal de SSO, falhas de logon, dentre outros.

2.7. 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.

2.8. O serviço de diretório da solução deve ter a capacidade de realizar a extensão de seu esquema através da configuração de atributos personalizados para atender requisitos de negócios complexos

2.9. O serviço de diretório da solução deve ser auto-escalável para suportar milhões de identidades e milhares de autenticações simultâneas.

2.10. Deve ter a capacidade de forçar a complexidade das senhas, minimamente para os seguintes requisito:

- a) • Tamanho mínimo.
- b) • Tamanho máximo.
- c) • Requerer mínimo de dígitos.
- d) • Requerer letras maiúsculas e minúsculas.
- e) • Requerer caracter especial (símbolo).
- f) • Limitar caracteres consecutivos.
- g) • Forçar expiração de senhas baseadas na idade das mesmas.
- h) • Guardar histórico de senhas para evitar reutilização

2.11. Prover notificação para expiração das senhas por email.

2.12. Capturar falhas de logon repetidas para bloqueio do usuário

2.13. A solução deve suportar adicionalmente a integração com serviços de diretório On-premisses e em nuvem, suportando minimamente:

- a) · Microsoft Active Directory.
- b) · Microsoft Azure AD
- c) · Google Directory
- d) · Diretórios LDAP

2.14. 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.

2.15. 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:

- a) Google.
- b) Facebook.
- c) LinkedIn.
- d) Microsoft.

2.16. 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.

2.17. 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.

2.18. O conector onpremisses 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 onpremisses deve englobar minimamente os seguintes componentes:

- a) Servidor RADIUS
- b) Cliente Radius
- c) Proxy reverso
- d) Integração com LDAP e Microsoft AD
- e) IWA, Integrated Windows Authentication

2.19. A solução deve 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.

2.20. A solução deve medir o risco da autenticação verificando o comportamento histórico da identidade através do conjunto dos seguintes atributos:

- 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.

- b) Geo Localização: medindo o risco da autenticação verificando sua localização geográfica do acesso atual em comparação com o seu comportamento usual.
- c) Dia da Semana: medindo o risco da autenticação verificando o dia da semana do acesso atual em comparação com seu comportamento usual.
- d) Horário do Acesso: mede o risco da autenticação verificando o horário do acesso atual em comparação com seu comportamento usual.
- e) Sistema Operacional: mede o risco da autenticação verificando o Sistema Operacional do acesso atual em comparação com seu comportamento usual
- 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

2.21. Deve prover a personalização das faixas de pontuação (0 a 100) para os administradores da solução para, no mínimo, as categorias:

- a) Sem risco
- b) Risco Baixo
- c) Risco Médio
- d) Risco Alto

2.22. 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;

2.23. 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:

- a) Requisitar múltiplos fatores de autenticação de forma dinâmica.
- b) Permitir o login sem o uso de múltiplos fatores.
- c) Negar a autenticação.

2.24. 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.

2.25. 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

2.26. 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.

2.27. Deve possuir integração com fontes de inteligência cibernética de terceiros reconhecidas no mercado, como, por exemplo, Palo Alto Cloud.

2.28. Deve possuir interface para envio de alertas de forma automatizada,

suportando, no mínimo:

- a) E-mail com conteúdo do alerta.
- b) Webhooks (ex: envio de mensagem para um canal do Microsoft Teams ou Slack).

2.29. Possuir dashboards pré-configurados com informações e gráficos com as seguintes características:

- a) Utilização do Motor de Análise do Comportamento dos Usuários.
- b) Comportamento dos usuários na utilização das aplicações.
- c) Visão sobre a segurança das aplicações.
- d) Mapa com a geolocalização das autenticações.
- e) Visão sobre o comportamento dos Endpoints (Mobile e Computadores).
- f) Visão sobre o comportamento das Identidades.

2.30. A solução deve permitir a configuração de dashboards personalizados.

2.31. Deve permitir o compartilhamento dos dashboards com outros usuários.

2.32. 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.

2.33. Deve registrar cliques de janela e textos utilizados durante a navegação do usuário final na aplicação monitorada.

2.34. Deve permitir ao administrador acessos a screen shots 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.

2.35. 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.

2.36. A solução não deve depender do uso de agentes para a gravação e monitoramento das sessões web, mas se utilizar estritamente de extensão instalada no browser, sem a necessidade de proxy ou utilização de jump servers. Tudo feita de maneira local no browser da estação de trabalho do usuário final.

2.37. 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.

2.38. Deve permitir gravação da sessões em nuvem, afim de não onerar espaço de armazenamento on premisses do órgão.

2.39. Deve permitir iniciar gravação, monitoramento contínuo e isolamento de sessão web por aplicação e perfil de acesso.

2.40. Deve alertar o usuário final de maneira visual, antes de iniciar o processo de monitoramento e gravação da sessão.

### **3. ITEM 2 - SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS - AUTENTICAÇÃO MULTI-FATOR ADAPTATIVA PARA IDENTIDADES DOS FUNCIONÁRIOS**

- 3.1. A solução deverá ser capaz de atender minimamente os seguintes casos de uso para requisitar um e mais fatores de autenticação:
- 3.2. Aplicações Web integradas nas funções de Logon único adaptativo para usuários - Single sign-on.
  - 3.2.1. Multi Fator de autenticação para soluções de VPN via RADIUS ou SAML.
  - 3.2.2. Qualquer dispositivo ou sistema operacional que suporte RADIUS.
  - 3.2.3. Plugin para ADFS (IDP, Identity Provider), Active Directory Federation Services.
  - 3.2.4. Sob demanda utilizando o protocolo OAuth e REST APIs.
  - 3.2.5. Para realizar o autosserviço de reset de senha ou desbloqueio de usuário.
- 3.3. A solução deverá ser capaz de oferecer minimamente os seguintes métodos para múltiplo fator de autenticação:
- 3.4. Usuário e senha dos diretórios suportados na solução.
- 3.5. Através de aplicativo para dispositivos móveis do tipo IOS e Android, oferecendo suporte para:
  - a) Biometria do tipo FaceID.
  - b) Biometria através do leitor de digital.
  - c) Smartphone push (Notificação para aprovar ou recusar uma autenticação).
  - d) Geolocalização abanque de dados de IPs.
  - e) Suporte a tokens OATH OTP.
  - 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.
- 3.6. Ligação telefônica requisitando um PIN previamente configurado.
- 3.7. 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.
- 3.8. Confirmação de código via email.
- 3.9. Clientes do tipo OATH OTP (exemplo, Google Authenticator).
- 3.10. Autenticadores que suportem FIDO2 / U2F, minimamente suportando:
  - a) Windows Hello.
  - b) Yubikey.
  - c) Google Titan Key
  - d) MacOS TouchID.
- 3.11. Perguntas e respostas previamente configuradas.
- 3.12. 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:

- a) Endereçamento IP.
- b) Dia da Semana.
- c) Datas específicas.
- d) Janelas de tempo entre duas datas.
- e) Janelas de tempo entre horários (exemplo, horário comercial).
- f) Tipo do Sistema Operacional.
- g) Tipo do Browser.
- h) Perfis configurados na solução.
- i) País que está sendo realizado o acesso.
- j) Se é um dispositivo gerenciado.
- k) Autenticação via certificado.
- l) Nível de Risco da autenticação medido por um motor de análise de comportamento dos usuários.

3.13. A solução deve ter capacidade de detectar casos de uso e perfis de autenticação já validados pelo 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.

3.14. O conjunto de fatores de autenticação disponibilizados devem ser baseados durante o acesso através de regras especificadas no item anterior e segregados por:

- a) Conjunto de aplicações.
- b) Um única aplicação.
- c) Regras para o autosserviço de reset de senha e desbloqueio de usuário.
- d) Portal do Administrador.
- e) Portal do Usuário.

3.15. A solução deve prover um portal WEB para o usuário final com as seguintes características:

- a) 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.
- b) Permitir o usuário redirecionar autenticação multi fator para outros usuários (desde que permitido).
- c) Permitir os usuários gerenciarem seus dispositivos registrados, minimamente:
- d) Smartphones Android e IOS.

3.16. Para cada dispositivo registrado, os usuários devem ter a capacidade de gestão de Realizar o auto registro de novos dispositivos móveis.

3.17. A solução deve prover um aplicativo móvel para Android e IOS com as seguintes características:

- 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 já integrado com os navegadores instalados nos dispositivos móvel.

b) Prover login através do scan de QRcode no portal web permitindo SSO sem identificação de usuário e senha.

c) Configurar OATH OTP adicionais provenientes de outras soluções.

d) Verificar dispositivos registrados (dispositivos móveis e sistemas operacionais).

e) Integração nativa com FaceID, TouchID, leitor biométrico dos dispositivos móveis alavancando os mesmos para autenticação biométrica durante login nas aplicações.

f) Reportar coordenadas GPS para os sistemas que utilizam geolocalização.

g) Detectar ROOT em dispositivos Android e Jailbreak em dispositivos IOS com a finalidade de detectar atividades maliciosas e como consequência o aplicativo é desabilitado para uso

3.18. 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:

a) Data e Hora.

b) Cidade / Geolocalização do acesso

c) Aplicação sendo acessada.

3.19. 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.

3.20. 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 multi fator. Este aplicativo dará suporte para casos onde não será possível o uso de um telefone celular / smartphone.

3.21. 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.

3.22. 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.

3.23. Medição de riscos, baseados em:

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.

b) Geo Localização: medindo o risco da autenticação verificando sua

localização geográfica do acesso atual em comparação com o seu comportamento usual.

c) Dia da Semana: medindo o risco da autenticação verificando o dia da semana do acesso atual em comparação com seu comportamento usual.

d) Horário do Acesso: mede o risco da autenticação verificando o horário do acesso atual em comparação com seu comportamento usual.

e) Sistema Operacional: mede o risco da autenticação verificando o Sistema Operacional do acesso atual em comparação com seu comportamento usual

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

3.24. Deve prover a personalização das faixas de pontuação (0 a 100) para os administradores da solução para, no mínimo, as categorias:

a) Sem risco

b) Risco Baixo

c) Risco Médio

d) Risco Alto

3.25. Deve prover para os administradores da solução a personalização da influência na medição do risco para cada atributo citado anteriormente. 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;

3.26. 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:

a) Requisitar múltiplos fatores de autenticação de forma dinâmica.

b) Permitir o login sem o uso de múltiplos fatores.

c) Negar a autenticação.

3.27. 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.

3.28. 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

3.29. 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.

3.30. Deve possuir integração com fontes de inteligência cibernética de terceiros reconhecidas no mercado, como, por exemplo, Palo Alto Cloud.

3.31. Deve possuir interface para envio de alertas de forma automatizada, suportando, no mínimo:

a) E-mail com conteúdo do alerta.

b) Webhooks (ex: envio de mensagem para um canal do Microsoft Teams ou Slack).

3.32. Possuir dashboards pré-configurados com informações e gráficos com as seguintes características:

a) Utilização do Motor de Análise do Comportamento dos Usuários.

b) Comportamento dos usuários na utilização das aplicações.

c) Visão sobre a segurança das aplicações.

d) Mapa com a geolocalização das autenticações.

e) Visão sobre o comportamento dos Endpoints (Mobile e Computadores).

f) Visão sobre o comportamento das Identidades.

#### **4. ITEM 3 - SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS - MONITORAMENTO COMPORTAMENTAL E MITIGAÇÃO DE RISCOS DAS IDENTIDADES PRIVILEGIADAS.**

4.1. A solução deve apoiar, no mínimo, os requisitos (artigos 6, 42, 43, 46, 48 e 50) da Lei Geral de Proteção de Dados-LGPD, como: Determinar como os dados deverão ser tratados, mantidos e protegidos e a quem responsabilizar em caso de descumprimento; Proteger o acesso a dados pessoais sensíveis; Responsabilizar pessoal e responder a incidentes; Aplicar 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.

4.2. Apoiando os requisitos da LGPD a solução deverá proteger e monitorar acessos a dados pessoais sensíveis por meio da segurança de credenciais e acessos de alto privilégio em serviços críticos, detectando e respondendo rapidamente a incidentes de segurança, identificando e mitigando ações privilegiadas com comportamentos de alto risco, avaliando riscos e testando a efetividade dos processos de proteção de dados por meio de relatórios da solução com identificação e classificação do status de risco do ambiente privilegiado, demonstrando conformidade e prova de que os controles de segurança necessários estão nos lugares certos, provendo análise comportamental, auditoria e segurança dos acessos a sistemas por meio de todas credenciais administrativas de alto privilégio em dispositivos e sistemas- alvo diversos do ambiente.

4.3. Um sistema-alvo da solução é definido como um servidor, uma estação de trabalho, um ativo de rede e de segurança, dentre outros mencionados a seguir, cujas credenciais de acesso passem a ser protegidas e gerenciadas pela solução;

4.4. Um usuário da solução é definido como qualquer pessoa que acesse um sistema-alvo mediante login na solução e uso de credenciais por ela gerenciadas.

4.5. Deve monitorar sessões, gravar, detectar, correlacionar e mitigar todos comportamentos anormais de, pelo menos, 50 usuários simultâneos acessando todos sistemas-alvo do ambiente tecnológico, dentre eles servidores Linux/Unix, Windows, controladores de domínio Microsoft Active Directory,

estações de trabalho Windows e demais ativos de rede e sistemas computacionais diversos.

4.6. A solução deverá ser entregue com acesso remoto seguro (externo a rede corporativa) para os usuários simultâneos mencionados, sem a necessidade de instalação e uso de clientes e VPN nos dispositivos dos usuários remotos por todo período de assinatura contratado.

4.7. A solução deverá ser entregue com acesso Single-sign-on e múltiplo fator de autenticação adaptativo para, no mínimo, os usuários internos e/ou remotos (externos a rede corporativa) mencionados, por todo período contratado, suportando, no mínimo:

4.8. Usuário e senha dos diretórios suportados, aplicativo para dispositivos móveis do tipo IOS e Android, oferecendo suporte para Biometria do tipo FaceID e através do leitor de digital, Smartphone push (Notificação para aprovar ou recusar uma autenticação), Geolocalização através de coordenadas GPS e banco de dados de IP, Suporte a tokens OATH OTP, autenticação na tela de login via QRcode sem a necessidade de digitar usuário e senha, com opção de forçar a biometria no dispositivo móvel, Entrega de código via SMS e chamada de voz, perguntas de segurança, notificações por e-mail e telefone celular, tokens OTP (on-line, off-line, por e-mail, hardware).

4.9. Autenticação auto-ajustada baseada no contexto de risco e segurança aprendidos pela solução, permitindo a criação de um perfil para cada usuário, aproveitando atributos históricos e situacionais específicos do mesmo, como localização, dispositivo, rede, horário e índice de risco de comportamento.

4.10. Análise de solicitações de autenticação em relação a padrões históricos, atribuição de índice de risco a cada tentativa de login, geração de alertas e criação de políticas de bloqueio a serem acionadas quando um comportamento anômalo é detectado e de acesso simplificado quando o usuário é entendido como legítimo.

4.11. Permitir que os usuários adicionem e modifiquem fatores de autenticação diretamente em um portal com definição de período de desvio do múltiplo fator de autenticação.

4.12. Prover relatórios e dashboards customizáveis com detalhamento de informações em tempo real sobre as atividades de autenticação, como falhas na autenticação secundária, tentativas bem-sucedidas de login e os fatores de autenticação mais usados.

4.13. Entenda-se como sistemas-alvo os baseados, em no mínimo, as seguintes tecnologias: S.O.: Linux/Unix e Microsoft Windows; Hypervisors: VMWare e Microsoft Hyper-V; Contas de usuários de sistemas e de serviço; Credenciais do Microsoft COM+, IIS, Apache TomCat, RedHat Jboss; Objetos (usuários, grupos e computadores) do Microsoft Active Directory e LDAP; Contas de usuários e administradores de bancos de dados Microsoft SQL Server, Oracle, PostgreSQL; Contas de equipamentos ativos de conectividade de redes LAN (Local Area Network) e WAN (Wide Area Network) - switches, roteadores, controladores/APs WiFi, SAN (Storage Area Network) e NAS (Network Attached Storage); Contas de usuários e administradores de consoles de gerenciamento de servidores e estações de trabalho; Contas de equipamentos dedicados à segurança, tais como Firewall, IPS, AntiSpam e filtros de conteúdo; Contas de equipamentos dedicados à segurança física, tais como câmeras de vigilância, catracas, etc; Credenciais de nuvem em VMWare ESXi, Azure, AWS, GCP, Office 365.

4.14. Gestão de dados do ciclo de vida e compartilhamento das contas privilegiadas, monitoramento e gravação de sessões privilegiadas:

4.15. A solução deve conceder acesso aos sistemas utilizando “Remote Desktop” e “SSH”, disponibilizados pelos sistemas-alvo do ambiente, sem que os usuários vejam qualquer senha e chave (vigentes no momento e providas para as aplicações e conexões remotas, devendo ser recuperadas de forma automática e transparente do repositório seguro de credenciais da solução), garantindo que não haja necessidade de instalação de aplicações e/ou agentes nas estações dos usuários para realizar o acesso a sistemas e 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 do usuário no S.O. 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;

4.16. A solução deve permitir Integração para gestão de acessos privilegiados em serviços de nuvem padrões de mercado, como Amazon Web Services (AWS), Google Cloud, IBM Cloud e Microsoft Azure, disponibilizando no mínimo as seguintes funcionalidades: Integração e gestão de acessos privilegiados em contas de serviços em nuvem; Integração com sessões de serviços de nuvem, incluindo início e finalização de sessão e Gravação e auditoria de acesso de sessões iniciadas em serviços de nuvem.

4.17. Deve possuir as sessões administrativas acessadas e monitoradas ao vivo, com compartilhamento de tela e controle de periféricos, como teclado e mouse (assistência remota), e por meio de gravação de comandos e vídeos das mesmas, em formato padrão de execução não proprietário da solução, possibilitando que os comandos e vídeos gerados possam ser indexados para pesquisa futura, permitindo o filtro de comandos e ações executadas ao longo da sessão gravada, possibilitando pesquisar ações específicas na sessão gravada;

4.18. Proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade da senha que incluem comprimento da senha (quantidade de caracteres), frequência de troca automatizada das senhas e chaves SSH, especificação de caracteres permitidos ou proibidos na composição da senha e outras medidas e mitigar problemas de segurança relacionados ao compartilhamento indevido de credenciais privilegiadas que são armazenadas localmente em dispositivos e também de contas que não são gerenciadas de forma centralizada por serviços de diretórios;

4.19. Descobrir credenciais privilegiadas referenciadas por serviços e processos automatizados e propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas e descobrir e alterar credenciais em ambiente Windows, incluindo contas nomeadas, administradores ‘built-in’ e convidados, para determinar movimentações laterais (pass-the-hash), exibidas em mapa de rede gráfico e interativo ou através de relatórios e interface de gerenciamento;

4.20. Gerenciar, de forma segura, senhas utilizadas por contas de serviço, evitando a utilização de senhas em texto claro por scripts ou rotinas dos equipamento e garantir a implementação dos privilégios mínimos necessários, provendo acesso às senhas das contas privilegiadas somente ao pessoal autorizado;

- 4.21. Deve proteger as senhas de credenciais administrativas locais de todas estações de trabalho Windows no repositório central seguro de credenciais, permitindo a aplicação de políticas granulares de rotações e trocas automáticas das senhas, trilha de auditoria dos acessos às mesmas, mitigando situações de roubo, perda e exploração de credenciais.
- 4.22. Quando as estações de trabalho não puderem estar conectadas de forma permanente ao repositório central de credenciais, deve aplicar, de forma autônoma, políticas de rotação de credenciais locais até a sincronização das mesmas definidas no repositório central da solução.
- 4.23. Possuir funcionalidade de “AD Bridge” para integração de servidores Linux/Unix no Active Directory, acompanhando a mesma nomenclatura e grupos do diretório LDAP ou AD;
- 4.24. Provisionar na plataforma Unix-like as contas e grupos do Active Directory que possuam permissão de acesso, de maneira automatizada e transparente;
- 4.25. Permitir a definição de Fluxos de Aprovação (Workflows) para obtenção de acesso às Contas Privilegiadas, com as seguintes características: Personalização de fluxos: permitir a configuração de fluxos para aprovação, de acordo com a criticidade e características da conta, e aprovação de, pelo menos, um responsável; Permitir a aprovação perante um agendamento de ações administrativas; ou seja; a aprovação do acesso ocorrerá em um dia, mas a liberação da senha ocorrerá de forma automática somente na data e horário previstos; Ser capaz de encontrar contas de usuários privilegiados que possam ser gerenciadas pela solução, permitindo ou não que a conta descoberta seja gerenciada pela solução; Ser capaz de substituir as senhas de identidades privilegiadas que estejam sendo utilizadas por determinado serviço em todos os locais onde estejam sendo utilizadas; A descoberta automática deve ser realizada por buscas no Active Directory (AD) e por intervalos de endereços IP;
- 4.26. Oferecer em sua aplicação web diferentes visões e opções de acordo com as permissões dos usuários, mostrando, por exemplo, apenas as funcionalidades delegadas àquele usuário; Suportar métodos para registrar e relatar qualquer ação realizada e detectada pela solução, incluindo registros de aplicações baseadas em texto, auditoria de banco de dados, aplicações syslog, notificações de e-mail;
- 4.27. Registrar cada acesso, incluindo os acessos via aplicação web, para solicitações de senha, aprovações, checkout's, mudanças de delegação, relatórios e outras atividades. Devem ser registrados os acessos à console de gerenciamento da solução, tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas; logoff dos usuários; Alterações nas funções de delegação; Adições, deleções e alterações de senhas gerenciadas pela solução; Operações das senhas dos usuários, incluindo check-in e check-out, solicitações negadas e permitidas; Os relatórios devem ser filtrados por período de tempo, tipo de operação, sistema, gerente e outros critérios;
- 4.28. Deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução, tais como: Lista de sistemas gerenciados; Senhas armazenadas; Eventos de alteração de senha; Permissões de acesso web; Auditoria de contas, sistemas e usuários; Alerta em tempo real;
- 4.29. Análise comportamental e mitigações de risco no ambiente crítico para Identidades Privilegiadas:

a) A solução deverá realizar a identificação e o correlacionamento de todas as ações citadas abaixo, montando perfis de comportamento gerais (usuários, acessos, credenciais, máquinas, outros) do ambiente privilegiado e acessos aos sistemas-alvo por meio da solução.

4.30. Deve combinar ações que caracterizam abusos, comportamentos anormais e fora dos padrões aprendidos/mapeados, aplicando ações mitigatórias automáticas como nova autenticação, suspensão e encerramento de sessões e troca das credenciais privilegiadas, em caso de atividades suspeitas de alto risco, detectando, no mínimo:

4.30.1. Acessos a solução:

a) Durante horários irregulares (quando um usuário recupera uma senha de conta privilegiada em uma hora irregular de acordo com seu perfil comportamental);

b) Durante dias irregulares (quando um usuário recupera uma senha de conta privilegiada em um dia irregular de acordo com seu perfil comportamental); 3.32.3 Através de IP irregular e desconhecido (quando um usuário acessa contas privilegiadas de um endereço IP ou sub-rede incomum, de acordo com seu perfil comportamental); não gerenciados (quando uma conexão com uma máquina é feita com uma conta privilegiada que não é gerenciada na solução).

4.30.2. Acessos gerais:

a) Excessivos a contas privilegiadas (quando um usuário acessa contas privilegiadas com mais frequência do que o normal, de acordo com seu perfil comportamental);

b) Anômalos a várias máquinas (quando uma conta efetuou login em um grande número de máquinas inesperadas durante um tempo relativamente curto);

c) Realizados fora da solução (diretamente no sistema-alvo);

d) Excessivos a uma máquina;

e) Usuários incomuns logando de uma máquina de origem conhecida;

f) Quando ocorrem indicações de atividade de um usuário inativo da solução;

g) Atividades definidas como suspeitas detectadas em sessões privilegiadas (comandos e anomalias na solução).

4.30.3. Máquinas:

a) Acessadas a partir de endereços IP incomuns;

b) Acessadas durante horários irregulares, de acordo com seu padrão de utilização;

c) Incomuns originando acessos.

d) Credenciais e Contas:

e) Suspeita de roubo de credenciais, quando um usuário se conecta a uma máquina sem primeiro recuperar as credenciais necessárias da solução;

f) Alteração de senha suspeita, quando é identificada uma solicitação para alterar ou redefinir uma senha ignorando a solução;

g) Credenciais expostas de contas de serviço que se conectam ao



LDAP em texto não criptografado;

h) Contas privilegiadas com configuração SPN (nome principal de serviço) vulneráveis a ataques de força bruta e de dicionário off-line, permitindo que um usuário interno malicioso recupere a senha de texto sem criptografia da contas;

i) Contas de serviço conectadas por meio de logon interativo.

4.31. Deve permitir a classificação de eventos por níveis de risco e respostas automáticas (suspensão e terminação de sessões) baseadas nos mesmos, com a possibilidade de colocar sessões em quarentena, pendentes de liberação e terminação pelo administrador.

4.32. Deve permitir a configuração de eventos críticos a serem reportados automaticamente, baseados em comandos Linux, comandos, janelas e aplicações Windows, expressões regulares para comandos em geral e eventos configurados manualmente, permitindo a atribuição de nível de risco customizado;

4.33. Arquitetura e Segurança da Solução:

a) Incorporar medidas de segurança como Certificação Common Criteria (CC) - ISO/IEC 15408 - como garantia de segurança do método utilizado no desenvolvimento do sistema de repositório seguro de credenciais e Criptografia dos módulos da solução, a fim de proteger a informação em trânsito entre módulos da solução e aplicações web dos usuários finais e possibilitar a utilização de criptografia do banco de dados utilizado pela solução para armazenar as credenciais gerenciadas pela mesma, sendo compatível com: AES com chaves de 256 bits, FIPS 140-2 e Encriptação PKCS#11 ou superior;

b) Deve utilizar banco de dados em alta disponibilidade, para armazenamento de credenciais, com as melhores práticas de segurança: mecanismo de blindagem do sistema operacional através da desativação ou desinstalação de serviços e portas de acesso não essenciais ao funcionamento da solução. Caso o banco de dados utilizado para armazenamento de credenciais seja de terceiros, a solução deverá ser entregue com licenças de software, garantia e suporte que o compatibilize com a solução;

c) Suportar a implementação em parque computacional Windows Server 2012 R2, Windows Server 2016 e/ou Linux em ambiente físico ou virtualizado com infra-estrutura (servidores/software em ambiente virtualizado, S.O., camada de balanceamento/redirecionamento de tráfego, etc) provida pela CONTRATANTE para implantação e uso da solução em alta disponibilidade;

d) A solução deverá possibilitar a sua instalação nos seguintes cenários: em diferentes provedores de nuvem, em diferentes regiões de um mesmo provedor de nuvem, entre provedores de nuvem e ambiente nas dependências da CONTRATANTE e em qualquer combinação entre os itens anteriormente descritos.

e) A solução deverá fazer uso dos serviços nativos de gestão de chaves dos provedores de nuvem para garantir o máximo nível de proteção de suas chaves criptográficas, suportando ao menos os provedores AWS e Azure.

f) A solução deverá possibilitar sua implantação de maneira automática, através da utilização de imagens ou pacotes de instalação

disponibilizados pelos provedores de nuvem, suportando ao menos os provedores AWS e Azure.

g) Os elementos críticos da solução, como Repositório Seguro de credenciais, Gateways de Gravação e Monitoração Comportamental deverão ser instalados em alta disponibilidade ativo-ativo em cada uma das localidades (site principal, site redundante adicional e nuvem), com chaveamento entre localidades (sites), garantindo que o processo seja transparente aos usuários conectados e a normalização das funcionalidades ocorra em até 5 (cinco) minutos, caso exista perda de comunicação e mecanismos para a recuperação de desastres compatível com soluções de backup e arquivamento disponíveis no mercado;

h) Prover, no mínimo, dois ambientes adicionais apartados da solução em produção para testes e homologação, replicando as mesmas licenças e funcionalidades do ambiente de produção.

#### 4.34. Proteção contra tomada de controle do Active Directory:

4.34.1. A solução deve monitorar todos os Controladores de Domínio Microsoft Active Directory e mitigar automaticamente situações como roubo de identidade, acesso não autorizado e ataques que visam a tomada de controle da rede via estrutura de diretórios, de acordo com as funções de monitoramento de atividades internas nos mesmos e tráfego de segmentos de rede que estes estejam instalados, para confirmação de integridade das solicitações e tickets Kerberos utilizados nos equipamentos e contas de usuário detectando, no mínimo:

a) Atividades anômalas em tempo real, típicas de ataques ao protocolo de autenticação Kerberos, como roubo de credenciais, movimentação lateral e escalonamento de privilégios;

b) A extração e uso de um Kerberos TGT (ticket de concessão de tickets) da memória LSASS (Subsistema de autoridade de segurança local) em um host para obter acesso a outros recursos da rede (Pass-the-ticket);

c) A recuperação e exploração de hashes de senha armazenados no banco de dados do SAM (Security Accounts Manager) ou do Active Directory para representar um usuário legítimo (Pass-the-Hash);

d) O uso do hash de uma conta de usuário para obter um ticket do Kerberos, que é usado para acessar outras contas e recursos de rede (Overpass-the-Hash);

e) A modificação das configurações de permissão de ticket do Kerberos para obtenção de acesso não autorizado aos recursos da rede - PAC Forjado (Manipulação de Certificado de Atributo de Privilégio);

f) Ataque ao Golden Ticket, quando busca-se a obtenção de acesso ao KDC (Kerberos Key Distribution Center) para geração de token principal de segurança que fornece acesso completo a um domínio inteiro;

g) A recuperação maliciosa de credenciais do controlador de domínio (DCSync);

h) Delegação não restrita, através da análise das contas de domínio, que recebem privilégios de delegação permissivos e, portanto, expõem o domínio a um alto risco;

- i) Manipulação de Certificado de Atributo de Privilégio - PAC Forjado, quando há a modificação das configurações de permissão de ticket do Kerberos para obtenção de acesso não autorizado aos recursos da rede.

## **5. ITEM 4 - SUBSCRIÇÃO PARA SOLUÇÃO DE SEGURANÇA PARA ARMAZENAMENTO DE CREDENCIAIS**

- 5.1. A solução deve prover extensão no Browser para capturar aplicações Web que utilizam formulário com usuário e senha e realizar o autopreenchimento do login e senha de forma automatizada. Estas informações devem ser guardadas de forma segura na solução para autopreenchimento nos futuros logins nestas aplicações.
- 5.2. A solução deve prover uma extensão de browser avançada somente para administradores da solução, com a finalidade de realizar o mapeamento dos campos dos formulários (em geral login e senha) para que depois de mapeados os administrados possam incluir como uma aplicação Web para SSO no catálogo geral, permitindo o SSO de aplicações que não suportam protocolos mais modernos como SAML , Oauth e OIDC.
- 5.3. Permitir o usuário de negócio/comum armazenar credenciais Web que não estão conectadas ao IDP / SSO, ou seja, diferentes das credenciais dos mesmos em um cofre pessoal na nuvem da solução e integrando com algum cofre on-premisses de soluções PAM de mercado.
- 5.4. Permitir o SSO das credenciais não conectadas ao IDP, removendo as credenciais do cofre em nuvem ou on-premisses e injetando as mesmas no formulário de login dessas aplicações web, facilitando a experiência de Login e mantendo um armazenamento seguro destas credenciais de negócio, estas credenciais nunca devem ser armazenadas ou com cache local no dispositivo do usuário final. A solução deve sempre consultar o cofre em nuvem ou on-premisses no momento da utilização da credencial.
- 5.5. Permitir o usuário de negócio/comum armazenar em cofre em nuvem ou on-premisses não somente de credenciais de aplicações web mas também credenciais de aplicações não web, tais como, SAP GUI, Emuladores de terminais etc.
- 5.6. Permitir o usuário de negócio/comum compartilhar de forma segura credenciais web, não web e notas seguras com parceiros de trabalho. Durante o compartilhamento o dono da credencial poderá definir uma faixa de tempo que ficará disponível a credencial e se o usuário que receberá acesso poderá visualizar ou não e editar a credencial.
- 5.7. Suportar o armazenamento seguro em cofre em nuvem ou on- premisses de notas seguras, tais como, senhas de wifi, números de cartões de crédito, dentro outras informações que devem ter um armazenamento seguro.
- 5.8. Permitir o usuário de negócio/comum que durante o login em uma aplicação web seja detectado o formulário de login e oferecer de forma automatizada a possibilidade de armazenar esta credencial em seu cofre pessoal, além de gravar a automação de login desta aplicação com a finalidade de facilitar a entrada na mesma nos subseqüentes logins, sem a necessidade de digitar suas credenciais novamente.
- 5.9. Permitir o administrador criar listas não autorizadas com endereços de websites, onde não seja oferecido para seu usuário comum / negócio a possibilidade de embarcar credenciais destes sites listados na mesma.

5.10. Permitir a transferência automatizada de custódia de credenciais para gerentes imediatos ou identidades configuradas pelo administrador de credenciais armazenadas e compartilhadas por usuário de negócio / comum, caso o mesmo seja desligado da empresa.

5.11. Toda o fluxo de transmissão das credenciais de negócio armazenadas em nuvem ou em cofre on-premises deve ser criptografado fim a fim (*end to end*) com a finalidade de manter a confidencialidade destas credenciais.

5.12. No momento do cadastro de uma credencial de negócio a solução via extensão do navegador deve sugerir senhas fortes baseadas em complexidade / entropia configuradas pelo usuário final.

5.13. A extensão de navegador da solução deve suportar minimamente, Microsoft Edge, Google Chrome e Firefox.

5.14. Permitir o administrador da solução configurar via perfis na solução quem poderá utilizar credenciais compartilhadas, por exemplo, redes sociais, sites de compras, dentre outros. Além de permitir o uso da credencial compartilhada toda a inteligência de automação de login (ingestão da credencial no formulário web de maneira automatizada) também deve ser compartilhado, desta forma o usuário final não necessita visualizar a credencial.

5.15. A solução deve permitir gerar relatórios detalhados de usuários que utilizaram as credenciais, compartilhamentos de credenciais, visualizações. Com minimamente as seguintes informações, quem utilizou, quando, qual credencial, com quem foi compartilhada e IP.

5.16. Deve possuir um aplicativo móvel para Android e iOS para armazenar credenciais de negócio de usuários finais em seu cofre pessoal, sendo estas credenciais acessíveis pelo aplicativo móvel, interface web e extensão do browser e totalmente sincronizadas independente de qual interface está sendo utilizada para acesso.

5.17. Quando usuário acessar um website e caso o mesmo possua uma credencial em seu cofre pessoal a extensão do navegador deve detectar e indicar no campo de login da aplicação de forma visual que o mesmo pode utilizar uma credencial armazenada em seu cofre pessoal. Nesta indicação visual no campo de login o usuário pode interagir com a mesma e selecionar a credencial a ser utilizada.

5.18. Deve ter a capacidade de importar credenciais (Usuário e Senha (automação de formulários de login)). de outros gerenciadores de senhas pessoais, minimamente suportando, LastPass, Keepass, Dashlane e Google.

## **6. ITEM 5 - SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS - PROTEÇÃO LOCAL PARA SERVIDORES WINDOWS**

6.1. As funcionalidades devem ser providas por meio de agentes instalados no sistema operacional dos servidores e permitir a proteção e controle dos privilégios.

6.2. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem ser através dos monitores/gravadores de acessos).

6.3. 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;

6.4. Exibir a reputação do arquivo executado advinda de, pelo menos, 1

(uma) fonte externa e disponibilizar a opção de encaminhamento de arquivo suspeito para análise de malware em soluções de mercado;

6.5. Suportar, no mínimo, as versões Windows Server 2003 SP2 x32 & x64, Windows Server 2008 x32 & x64, Windows Server 2008 R2 x64, Windows Server 2012/2012 R2, Windows Server 2016 e Windows Server 2019;

6.6. 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.

6.7. 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.

6.8. 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.

6.9. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina.

6.10. Fazendo uso das funcionalidades instaladas no sistema operacional alvo, deve 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.

6.11. Implementar a verificação de checksum do arquivo, dos parâmetros permitidos e da assinatura de fabricante, para objetos reutilizáveis da solução.

6.12. Implementar o suporte ao nome exato da aplicação/arquivo/script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução.

6.13. Utilizar eventos reportados na interface da ferramenta para criação de novas políticas ou incluí-los em políticas existentes.

6.14. 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.

6.15. Impedir a desativação das funcionalidades instaladas no sistema operacional alvo sem autorização e/ou registro da atividade por meio da interface de gerência.

6.16. Disponibilizar o registro das execuções e atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido.

6.17. Monitorar e exibir acessos e atividades realizadas na própria solução.

6.18. Deve permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras, individualmente ou em grupos.

6.19. 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.

6.20. Deve verificar a reputação dos arquivos executados e detectados pelas funcionalidades instaladas no sistema operacional alvo ou órgãos de controle de ameaças, como por exemplo o VirusTotal.com ou similares.

- 6.21. Deve permitir a execução automática de tipos desconhecidos de arquivo, de acordo com sua origem, mesmo possuindo restrições.
- 6.22. Possibilitar o monitoramento e a criação de evidência em vídeo de certas execuções de arquivo e de execuções sob certas condições definidas em política.
- 6.23. Possibilitar ao usuário final a solicitação de liberação de atividades específicas fazendo uso das funcionalidades instaladas no sistema operacional alvo.
- 6.24. Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line.
- 6.25. 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.
- 6.26. Oferecer monitoramento de atividade maliciosa dos processos em execução, visando detectar tentativas de roubo de credenciais.
- 6.27. Fazendo uso das funcionalidades instaladas no sistema operacional alvo, a solução deve alertar, reportar e bloquear atividade anômala de arquivos e usuários durante a interação com bases de senhas no formato hash, como por exemplo, SAM local e LSASS.
- 6.28. 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.
- 6.29. Permitir o envio de arquivos suspeitos, executados sob sua supervisão, para soluções de análise de ameaça do tipo Sandbox.
- 6.30. Possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados;
- 6.31. Permitir criar uma whitelist, onde é configurado todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista automaticamente seja bloqueada.
- 6.32. Possuir uma integração com Windows UAC, e conter relatórios do uso de prompts aos usuários feitos pelo UAC
- 6.33. Suportar a guarda de políticas de hosts que não façam parte do Active Directory
- 6.34. Manter todas as políticas em cache e serem aplicadas ao endpoint, ainda que o mesmo não esteja conectado à rede corporativa
- 6.35. Deve permitir que mensagens customizadas sejam mostradas antes que uma aplicação seja executada ou bloqueada
- 6.36. Deve suportar adição múltiplas mensagens, estas mensagens devem possibilitar edição e suportar múltiplas linguagens
- 6.37. Deve possuir capacidade de relatórios de aplicações e eventos de usuários inclusos na solução
- 6.38. Realizar varredura e inventário de aplicações instaladas no sistema operacional.
- 6.39. Deve permitir a configuração de “iscas”, como senhas e credenciais falsas de administrador local para detecção de ataques em andamento e

bloqueio proativo.

## **7. ITEM 6 - SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS - PROTEÇÃO LOCAL PARA SERVIDORES LINUX/UNIX**

- 7.1. As funcionalidades devem ser providas por meio de agentes instalados no sistema operacional dos servidores e permitir a proteção e controle dos privilégios em contas de usuário em equipamentos Unix, Linux, Solaris e AIX e associar os privilégios e comandos controlados às contas cadastradas no repositório seguro de credenciais, realizando o controle no próprio sistema operacional.
- 7.2. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem passar pelos monitores/gravadores de acessos) fazendo uso das funcionalidades instaladas no sistema operacional alvo.
- 7.3. 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.
- 7.4. Implementar restrições, em uma plataforma, de maneira global ou em uma conta de usuário ou grupo de maneira granular.
- 7.5. Realizar o controle mediante interceptação do comando antes que ele seja executado, permitir a liberação de comandos privilegiados a usuários comuns, permitir que os comandos executados em sistemas monitorados sejam gravados em modo texto no repositório seguro de credenciais, permitir o agrupamento de comandos, bem como a utilização de coringas como (\*), para uma definição ampla de parâmetros.
- 7.6. Permitir que sejam atribuídas permissões para usuários e grupos, inclusive do Active Directory e 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.
- 7.7. 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.
- 7.8. Possibilitar o uso da máscara de usuário na execução dos comandos (valores entre 0000 e 0777).
- 7.9. 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.
- 7.10. Disponibilizar a funcionalidade de restrição de Shell, que impossibilite que scripts e shells de sistema executem comandos não permitidos pelas regras definidas na solução.
- 7.11. Monitorar e exibir acessos e atividades realizadas no próprio sistema
- 7.12. Possibilitar mapear e coletar atividades regulares de usuários através do modo observação, agregando e exportando os resultados para um perfil.
- 7.13. Prover um controle de comandos completo, com a possibilidade de criar uma lista de comandos permitidos e bloqueados (whitelisting/blacklisting), a serem alterados (criação de aliás) ou prevenir que comandos sejam

executados ou permitir trabalhar em Shell modificado/controlado;

7.14. Prover meios de permitir que os usuários executem comandos específicos e conduzam sessões remotamente baseado em regras sem autenticar-se diretamente utilizando credenciais privilegiadas.

## **8. ITEM 7 - SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS - PROTEÇÃO LOCAL PARA ESTAÇÕES DE TRABALHO**

8.1. As funcionalidades devem ser providas por meio de agentes instalados no sistema operacional das estações de trabalho e permitir a proteção e controle dos privilégios.

8.2. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem ser através dos monitores/gravadores de acessos).

8.3. 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;

8.4. Exibir a reputação do arquivo executado advinda de, pelo menos, 1 (uma) fonte externa e disponibilizar a opção de encaminhamento de arquivo suspeito para análise de malware em soluções de mercado;

8.5. Suportar, no mínimo, as versões de estações de trabalho: Windows XP SP3, Windows Vista SP1, Windows 7 x32 & x64, Windows 8/8.1 x32 & x64, Windows 10 x32 & x64;

8.6. 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.

8.7. 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.

8.8. 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.

8.9. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina.

8.10. Fazendo uso das funcionalidades instaladas no sistema operacional alvo, deve 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.

8.11. Implementar a verificação de checks um do arquivo, dos parâmetros permitidos e da assinatura de fabricante, para objetos reutilizáveis da solução.

8.12. Implementar o suporte ao nome exato da aplicação/arquivo/script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução.

8.13. Utilizar eventos reportados na interface da ferramenta para criação de novas políticas ou incluí-los em políticas existentes.



- 8.14. 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.
- 8.15. Impedir a desativação das funcionalidades instaladas no sistema operacional alvo sem autorização e/ou registro da atividade por meio da interface de gerência.
- 8.16. Disponibilizar o registro das execuções e atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido.
- 8.17. Monitorar e exibir acessos e atividades realizadas na própria solução.
- 8.18. Deve permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras, individualmente ou em grupos.
- 8.19. 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.
- 8.20. Deve verificar a reputação dos arquivos executados e detectados pelas funcionalidades instaladas no sistema operacional alvo ou órgãos de controle de ameaças, como por exemplo o VirusTotal.com ou similares.
- 8.21. Deve permitir a execução automática de tipos desconhecidos de arquivo, de acordo com sua origem, mesmo possuindo restrições.
- 8.22. Possibilitar o monitoramento e a criação de evidência em vídeo de certas execuções de arquivo e de execuções sob certas condições definidas em política.
- 8.23. Possibilitar ao usuário final a solicitação de liberação de atividades específicas fazendo uso das funcionalidades instaladas no sistema operacional alvo.
- 8.24. Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line.
- 8.25. 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.
- 8.26. Oferecer monitoramento de atividade maliciosa dos processos em execução, visando detectar tentativas de roubo de credenciais.
- 8.27. Fazendo uso das funcionalidades instaladas no sistema operacional alvo, a solução deve alertar, reportar e bloquear atividade anômala de arquivos e usuários durante a interação com bases de senhas no formato hash, como por exemplo, SAM local e LSASS.
- 8.28. 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.
- 8.29. Permitir o envio de arquivos suspeitos, executados sob sua supervisão, para soluções de análise de ameaça do tipo Sandbox.
- 8.30. Possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados;
- 8.31. Permitir criar uma whitelist, onde é configurado todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista

automaticamente seja bloqueada.

8.32. Possuir uma integração com Windows UAC, e conter relatórios do uso de prompts aos usuários feitos pelo UAC

8.33. Suportar a guarda de políticas de hosts que não façam parte do Active Directory

8.34. Manter todas as políticas em cache e serem aplicadas ao endpoint, ainda que o mesmo não esteja conectado à rede corporativa

8.35. Deve permitir que mensagens customizadas sejam mostradas antes que uma aplicação seja executada ou bloqueada

8.36. Deve suportar adição múltiplas mensagens, estas mensagens devem possibilitar edição e suportar múltiplas linguagens

8.37. Deve possuir capacidade de relatórios de aplicações e eventos de usuários inclusos na solução

8.38. Realizar varredura e inventário de aplicações instaladas no sistema operacional.

8.39. Deve permitir a configuração de “iscas”, como senhas e credenciais falsas de administrador local para detecção de ataques em andamento e bloqueio proativo.

## **9. ITEM 8 - SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS - PROTEÇÃO PARA APLICAÇÕES CONTEINERIZADAS**

9.1. A solução deve prover proteção e gerenciamento de secrets que atenda as demandas de segurança de credenciais e suas subcategorias, onde entende-se como secret uma estrutura de dados que possa conter senhas, chaves privadas, tokens e chaves de APIs e ser entregue de maneira segura e criptografada para aplicações, contêineres e serviços.

9.2. Deve suportar, no mínimo, 1 cluster de orquestradores de contêineres com hosts distribuídos e aplicações rodando e deve ser totalmente compatível para funcionamento em ambiente Docker, instalado em modo contêiner, sendo esse executado em diversas plataformas, incluindo, mas não se limitando a Windows e Linux, permitir integração nativa com as seguintes plataformas: Openshift versão 3.11 ou superior (com Docker registry instalado) e oferecer integração com ferramentas de gerenciamento de configuração, suportando minimamente: Chef, Puppet, Ansible e Terraform.

9.3. Deve rodar dentro de containers intermediando as chamadas e o acesso seguro dos pods às secrets guardadas na solução possuir interface Web com dashboard ou interface gráfica que exiba o estado operacional (system health) relativo aos componentes da solução, incluindo réplicas e componentes de balanceamento de carga e demonstrar graficamente o relacionamento entre diferentes entidades (secrets, usuários e grupos, usuários e grupos sistêmicos).

9.4. Deve criptografar todas as chaves privadas SSL utilizadas por quaisquer serviços da solução, ou utilizadas na criptografia da base de dados evitando que sejam armazenadas em texto claro no sistema de arquivos. A criptografia deve ocorrer antes da escrita em armazenamento persistente, evitando que informações sejam comprometidas em caso de acesso aos dados. Deve permitir que a chave master de criptografia seja armazenada e provida por soluções de HSM.

9.5. A solução deverá atuar como gerador e intermediário (broker) de secrets para diversos clientes, como aplicações, contêineres e clientes de

criptografia e possibilitar o armazenamento de múltiplas versões de um mesmo secret. O fornecimento de secrets deve oferecer meios de controle de solicitante com múltiplos fatores, incluindo minimamente Tempo de vida (TTL) e restrições de IP/range.

9.6. Os secrets devem ser modificáveis, com base em critérios de tempo de uso (Lease time) ou expiração, sendo que após expiração, a rotação ocorre de acordo com políticas definidas no sistema. Todo secret deve conter por padrão, pelo menos duas listas de acesso: Papéis/grupos que podem ler o secret e que podem alterar o secret.

9.7. Além do controle de concessão dos secrets, deve haver meios de revogar totalmente o acesso a um secret sob demanda ou via política. Para evitar acessos excessivos ou não autorizados a um secret, a solução deverá disponibilizar meios de abstrair a gerência e acesso aos secrets, minimizando o acesso direto e as chamadas de APIs.

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

9.9. As operações com secrets devem gerar trilha de auditoria contendo, no mínimo: Identificação do cliente (usuário ou usuário sistêmico), Identificação do secret, Horário (Timestamp completo), Ação (leitura ou alteração) e se a ação foi permitida ou não.

9.10. Deve obedecer uma configuração inicial estrita de “negação padrão” para acesso aos secrets, onde cada requisitante deve ser previamente autorizado via política de segurança, que identifique a aplicação ou usuário solicitante como membro de um grupo com autorização de acesso ou solicitação do secret em questão.

9.11. Deve utilizar definição de papéis (RBAC) para autorização de identidades de usuários e de aplicações onde possam ser definidos e relacionados entre si quando possível: Usuários, Grupos de usuários, Usuários sistêmicos (máquinas, serviços e processos) e Grupos de usuários sistêmicos.

9.12. A definição de usuários sistêmicos deve suportar máquinas estáticas e máquinas distribuídas por ferramentas de orquestração (Host Factory), provendo assim suporte à ambientes elásticos.

9.13. O relacionamento com os secrets entre usuários sistêmicos ou não, deve ser realizado por meio de políticas de uso e acesso, que definirão Usuários que poderão acessar a ferramenta via interface gráfica, Linha de comando (CLI) ou APIs, e seus privilégios; Máquinas (usuários sistêmicos) que poderão acessar a ferramenta de maneira programática e obter dados, e suas permissões em dados protegidos, inclusive secrets; Variáveis que representam secrets armazenados e quem terá acesso a eles; Webservices que possam prover serviços a solução e seus acessos.

9.14. Quando a solução operar em integração com Kubernetes e Openshift, deve permitir que os seguintes recursos sejam definidos como usuários sistêmicos: Namespace, Deployment, Deployment Config (apenas Openshift), Stateful Set, Service Account e Pod e suportar integração e uso do Kubernetes Authenticator Client (K8S), em modo Init ou Sidecar.

9.15. Todas as operações envolvendo usuários e grupos sistêmicos e não-sistêmicos, políticas e secrets, incluindo a criação, leitura e alteração, devem ser

feitas via linguagem aberta de serialização YAML.

9.16. A obtenção de secrets deve ser permitida por diversos meios, incluindo, pelo menos, linha de comando (CLI) e RestAPI. Os secrets deverão ser disponibilizados unicamente para as aplicações ou serviços que os consomem, sendo que em hipótese alguma, devem ser disponibilizados no nível do sistema operacional ou “namespaces” acessíveis por outras aplicações.

9.17. Visando a facilidade de integração com aplicações existentes ou com práticas de desenvolvimento vigentes, a solução deve fornecer bibliotecas de integração em linguagens variadas, incluindo minimamente .NET, Java, Ruby e Go.

9.18. Para que a disponibilização de secrets seja operacionalizada em diversos ambientes, deve fornecer ferramenta que leia os arquivos YAML e realize a injeção do conteúdo dos secrets em variáveis de ambiente do processo selecionado, que serão automaticamente eliminadas quando o processo for finalizado. A ferramenta de leitura e solicitação de secrets via YAML deve ser compatível com outros provedores de secret, pelo menos, AWS S3, AWS Secrets Manager, Chef Data Bags, GoPass, keyrings e Keepass kdbx database files.

9.19. A solução deverá guardar e rotacionar os secrets no repositório central de credenciais da solução (item 1 desta especificação técnica), sem necessidade de criação de novo ambiente de administração de credenciais, mantendo os mesmos requisitos de segurança já definidos para aquela solução.

9.20. Deve oferecer recursos de redundância, alta disponibilidade e suporte a balanceamento de carga se utilizando da infra-estrutura disponibilizada pela CONTRATANTE. A alta disponibilidade deve conter funcionalidade de replicação automática entre as bases da solução, oferecendo pelo menos 2 réplicas. O conjunto de réplicas deve oferecer funcionalidade de Failover automático, onde uma das réplicas assumirá a operação em caso de problemas. Deve haver funcionalidade de backup seguro do conteúdo armazenado e configurações do produto, possibilitando a prática de Disaster Recovery.

9.21. Para que não haja sobrecarga nem exposição do repositório central da solução e suas redundâncias, a solução deve oferecer componentes que absorvam a carga de requisições. Esses componentes devem agregar capacidade de requisições por segundo de maneira quantitativa ao total da solução.

9.22. Prover, no mínimo, dois ambientes adicionais externos da solução em produção para testes e homologação, replicando as mesmas licenças e funcionalidades do ambiente de produção.

9.23. A solução deverá ser entregue com licença equivalente ao padrão enterprise sem restrição a volume de dados trafegados ou gerados, que não impossibilite a replicação e redundância (alta disponibilidade); ou que possua quaisquer outras limitações características de soluções não corporativas ou incompatíveis com o parque tecnológico da CONTRATANTE.

## **10. ITEM 9 - SOLUÇÃO DE SEGURANÇA PARA IDENTIDADES E ACESSOS - PROTEÇÃO PARA APLICAÇÕES**

10.1. A solução deve ser disponibilizada com um SDK (Software Development Kit) que pode ser configurado para permitir que aplicações possam:

a) Solicitar as credenciais sob demanda ao invés de utilizar credenciais

estáticas;

b) Atualizar informações de contas automaticamente no banco de dados de senhas;

c) Inscrever automaticamente em sistemas alvo sem aguardar por atualizações dinâmicas;

d) Alterar senhas em texto-claro incorporados em aplicações de uma forma segura no banco de dados de senhas;

e) Solicitar as credenciais sob demanda via REST ou SOAP ao invés de utilizar credenciais estáticas;

f) Atualizar informações de contas automaticamente no banco de dados de senhas;

g) Deverá integrar-se nativamente ao cofre digital da solução, utilizando sua mesma interface web.

10.2. A solução deverá possuir mecanismo de segurança que mantenha a entrega de credenciais em caso de queda da rede ou parada total do cofre digital, evitando assim a parada de aplicações críticas.

10.3. A solução deverá fornecer as senhas pelo menos via consulta de rede ou Webservice.

10.4. O uso de agente deve permitir instalação em múltiplos servidores web, sem necessidade de aquisição de licenças, visando fornecer a melhor adaptação à arquitetura do contratante.

10.5. Deverá manter um cache atualizado das credenciais utilizadas localmente no servidor da aplicação, a fim de prevenir falhas na comunicação com o cofre digital e trazer velocidade às consultas

10.6. O cache deverá ser atualizado periodicamente com possibilidade de configuração da frequência de atualização.

10.7. Deverá suportar a utilização de executável para scripts e aplicações nativas em plataforma Windows

10.8. Deverá suportar a utilização de integração com servidores WebSphere, WebLogic, JBoss e Tomcat, para fornecimento de credenciais via data sources, ou de funcionalidade semelhante.

10.9. Deverá suportar a autenticação de aplicações que consultam credenciais, permitindo definir o caminho da aplicação, usuário da solução operacional, endereço do servidor e hash MD5 do código ou de funcionalidade semelhante

10.10. Deverá suportar redundância de credenciais, oferecendo mais de um usuário e senha à aplicação em questão de maneira transparente, de forma que se evite qualquer possível indisponibilidade mínima durante o processo de troca de senhas.

## **11. ITENS 10 E 14 - SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DAS SOLUÇÕES (POR ITEM / MÓDULO)**

11.1. Os equipamentos concentradores, softwares e o Sistema de Gerência Centralizada devem ser instalados no Ministério da Cultura, Brasília-DF.

11.2. Reunião inicial: deverá ser realizada uma reunião inicial entre o gestor do contrato e a CONTRATADA, cuja pauta observará, pelo menos:

a) Assinatura da Carta de Confidencialidade;

- b) Carta de Apresentação do Preposto;
- c) Esclarecimentos relativos a questões operacionais e de gerenciamento do contrato;
- d) Estrutura organizacional da CONTRATANTE;
- e) Infraestrutura de TI da CONTRATANTE;

11.3. A CONTRATADA deverá prestar serviços de instalação e configuração, que compreendem, entre outros, os seguintes procedimentos:

- a) Análise da topologia e arquitetura da rede existente do Ministério da Cultura;
- b) Análise dos acesso Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;
- c) Soluções de segurança existentes e aplicáveis à solução ofertada;
- d) Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;
- e) Apresentação do plano de implantação com o descritivo de todos os serviços a serem executados e topologia física e lógica a ser implementada;

11.4. O serviço de instalação e configuração da solução de segurança para identidades e acessos consiste em uma série de etapas detalhadas para garantir a implantação bem-sucedida e o correto funcionamento da solução na infraestrutura da organização.

11.5. O prazo máximo para entrega da solução será de 45 (quarenta e cinco) dias corridos, a contar da assinatura do contrato entre o órgão e a Contratada.

11.6. Antes de findar qualquer um dos prazos fixados, o fornecedor poderá formalizar, de forma devidamente fundamentada, pedido de sua prorrogação, cujas razões expostas serão examinadas pelo Ministério da Cultura, que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas, observando disposto legais.

11.7. Será fornecido o “Terno de Recebimento Provisório”, no prazo de 10 (dez) dias corridos, contados do primeiro dia imediatamente posterior ao recebimento da comunicação da empresa informando que a atualização da licença (suporte e subscrição) foi homologada no website da fabricante, para efeito de posterior verificação da conformidade do produto com as especificações e com a proposta, e desde que não haja pendências de responsabilidade da empresa;

11.8. E será emitido o “Termo de Recebimento Definitivo”, no prazo máximo de 5 (cinco) dias corridos, contados da emissão do Termo de Recebimento Provisório e após o atendimento de todas as eventuais solicitações da contratante.

11.9. O serviço de instalação e configuração será demandado em separado para cada um dos módulos, devendo contemplar as etapas:

11.9.1. **Levantamento de Requisitos:** Inicialmente, uma equipe de especialistas realizará um levantamento detalhado dos requisitos específicos da organização. Será feita uma análise minuciosa das necessidades de segurança, dos sistemas e aplicativos a serem integrados, dos tipos de acessos e

permissões requeridos, e dos cenários de uso da solução.

11.9.2. **Planejamento:** Com base nos requisitos levantados, será elaborado um plano de instalação e configuração que descreva as etapas, recursos, prazos e responsabilidades envolvidas no projeto. O planejamento incluirá a definição da arquitetura da solução, a seleção de componentes e a infraestrutura necessária.

11.9.3. **Preparação do Ambiente:** Antes da instalação da solução, o ambiente de TI da organização será preparado para receber a nova infraestrutura. Isso pode incluir a atualização de sistemas operacionais, a configuração de servidores e a instalação de pré-requisitos necessários para a solução.

11.9.4. **Instalação dos Componentes:** Os componentes da solução serão instalados nos servidores e dispositivos designados. Esse processo pode incluir a instalação de servidores de autenticação, servidores de diretórios, servidores de aplicação, bancos de dados e outros componentes relevantes para o funcionamento da solução.

11.9.5. **Configuração de Parâmetros:** Uma vez instalada, a solução será configurada com os parâmetros adequados de acordo com os requisitos da organização. Serão definidas políticas de acesso, níveis de privilégios, autenticação multifator, entre outras configurações específicas para garantir a segurança e conformidade.

11.9.6. **Testes e Validação:** Após a instalação e configuração, serão realizados testes abrangentes para garantir que a solução esteja funcionando conforme o esperado. Serão feitos testes de autenticação, de autorização, de auditoria, entre outros, para verificar a eficácia e eficiência da solução.

11.10. **Após a instalação de cada um dos respectivos módulos, a CONTRATADA deverá providenciar Entrega e Documentação:** ao final do processo, toda a documentação referente à instalação e configuração será entregue à organização, incluindo manuais de uso, políticas de segurança, procedimentos de administração e outros documentos relevantes.

11.11. Com a conclusão dessas etapas, a organização contará com uma solução de segurança para identidades e acessos devidamente instalada e configurada, pronta para garantir a proteção dos ativos digitais e a conformidade com as regulamentações aplicáveis. O serviço de instalação e configuração deverá assegurar que a solução seja adequadamente integrada à infraestrutura existente, garantindo a eficácia, eficiência, efetividade e economicidade dos processos de gerenciamento de identidades e acessos.

## 12. ITENS 11 E 15 - SERVIÇO DE TREINAMENTO / CAPACITAÇÃO

12.1. A CONTRATADA deverá repassar à CONTRATANTE todas as informações solicitadas e documentação da solução, além de disponibilizar treinamento conforme especificações a seguir.

12.2. O treinamento a ser fornecido pela CONTRATADA deverá abranger diversos aspectos da solução contratada, com o objetivo de educar e capacitar as equipes técnicas do CONTRATANTE a operar, configurar, administrar e resolver problemas usuais na solução adquirida, englobando tanto os componentes de hardware quanto de software. De forma a desenvolver habilidades necessárias para operar e gerenciar efetivamente a solução.

12.3. O treinamento deve ser adaptado às necessidades específicas da organização, considerando o escopo da solução contratada e os papéis das

peças que participarão do treinamento. Ele deve incluir sessões teóricas e práticas, para garantir um entendimento completo das funcionalidades e operação da solução.

12.4. O treinamento será demandado à CONTRATADA pela CONTRATANTE após a emissão do Termo de Recebimento Definitivo (TRD) do respectivo item contratado.

12.5. O treinamento deverá ser em Brasília - DF, para a equipe técnica do CONTRATANTE.

12.5.1. Podendo ser ofertado forma **remota e síncrona** para os participantes indicados pelo Ministério da Cultura.

12.5.2. A CONTRATADA deverá apresentar com antecedência a ementa do treinamento.

12.6. Deverá ser ofertada para 1 (uma) turma com no máximo 10 alunos e com carga horária mínima de 12h.

12.6.1. Os horários do curso deverão seguir a conveniência do CONTRATANTE, podendo sua realização ocorrer apenas em um dos períodos do dia (manhã ou tarde), quatro (04) h por dia.

12.6.2. As datas dos treinamentos serão acordadas entre o órgão e CONTRATADA, e formalizada em Ordem de Serviço.

12.7. Deverá ser fornecido material didático completo e com conteúdo oficial do fabricante.

12.7.1. Materiais disponibilizados no formato de Educação a Distância (EaD) assíncronos não serão contabilizados como carga-horária.

12.7.2. Deverá ser fornecido certificado de conclusão emitido pelo fabricante.

12.8. Todos os custos relativos à realização do treinamento são de exclusiva responsabilidade da CONTRATADA.

### **13. ITENS 12 E 13 - SERVIÇO DE ACESSO REMOTO CONFIANÇA ZERO (ZTNA) / SERVIÇO DE ACESSO SEGURO INTERNO/EXTERNO (SWG)**

13.1. A prestação de serviço deverá contemplar uma plataforma de segurança a ser fornecida na modalidade de licenciamento em nuvem e possuir aderência com o conceito Security Service Edge, com as seguintes capacidades em nuvem:

13.1.1. **ZTNA:** Acesso remoto seguro baseado no conceito Zero Trust Network Access, garantindo sempre o menor privilégio de acesso a aplicações posicionadas no Datacenter do Ministério da Cultura; e

13.1.2. **Secure Web Gateway:** Proteção em tempo real em que a solução atua como um controlador do acesso entre o usuário e recurso remoto.

13.2. **Características Gerais:**

13.2.1. A solução de segurança proposta deverá englobar:

13.2.1.1. Acesso Remoto às aplicações: A solução de ZTNA deverá prover acesso seguro e controlado baseado nos protocolos TCP e UDP a aplicações privadas do Ministério da Cultura (MinC) através de cliente do próprio fabricante instalado na máquina;

13.2.1.2. Proxy em nuvem: processamento do tráfego web dos usuários em tempo real com destino ao Microsoft Office 365, AWS, Aplicações SaaS



não sancionadas, Filtro URL, Proteção contra domínios maliciosos, aplicações indesejadas e por fim análise e prevenção contra malwares.

13.2.2. A solução proposta deverá ser fornecida em uma arquitetura 100% baseada em nuvem, através do posicionamento de, no mínimo, 2 (duas) estruturas de processamento redundantes no território nacional posicionados em cidades distintas.

13.2.3. A Solução deverá prover às redes remotas 2 endereços Ips exclusivos para acesso a internet, saindo apenas com Ips designados para o Brasil. Esta funcionalidade também deverá garantir que os endereços IPs alocados não sejam compartilhados com outros clientes.

13.2.4. Em caso de falha dos datacenters posicionados em território nacional a plataforma deverá garantir o uso de quaisquer outros datacenters no mundo, devendo ser provisionado é incluso no licenciamento caso se faça necessário.

13.2.5. A licença ofertada para atendimento ao referencial técnica não deverá possuir volume mínimo por usuário/mês, ou seja, deverá ser ilimitado.

13.2.6. O fabricante deverá possuir registro público garantindo disponibilidade de 5 Nove (99.999%) das estruturas de datacenter.

13.2.7. A solução SSE deverá estar licenciada para, no mínimo, 450 túneis seguros

13.2.8. Possuir peering com os principais provedores SaaS/IaaS, dentre eles: Amazon, Microsoft, Google, Akamai, Cloudflare e Oracle Cloud;

13.2.9. Possuir painel de gestão único e centralizado, garantindo visibilidade de todos os módulos propostos para o serviço SASE/SSE, dentre eles: Secure Web Gateway e ZTNA.

13.2.9.1. O acesso deverá ser através de um único IP fixo dedicado,

13.2.9.2. O IP dedicado não podendo ser modificado sem aviso prévio à CONTRATANTE.

13.2.10. Toda a parte de gestão deverá ser centralizada em uma única console, garantindo a aplicação das políticas criadas em todos os datacenters disponíveis pelo fabricante e independente de qual data center o usuário utilize, a política estará vigente para proteção e controle do tráfego.

13.2.11. A solução deverá registrar os logs transacionais relacionados a solução de Secure Web Gateway e estes deverão ser encaminhados para a solução de SIEM de propriedade do Ministério da Cultura;

13.2.11.1. Entende-se por log transacional o registro de evento feito de modo cru e não normalizado pela solução.

13.2.12. A plataforma deve permitir a criação de diferentes perfis de acesso a console de administração com, no mínimo, as seguintes possibilidades:

a) Perfil de administrador geral: acesso total às funções da solução, acesso aos logs de auditoria dos outros usuários, criação e administração de outras contas de acesso;

b) Perfil de administrador intermediário: acesso total às funções da solução, exceto criação e administração de outras contas de acesso;

c) Perfil de Cibersegurança: acesso ao painel para análise de ameaças encontradas pela solução.

13.2.13. A solução deverá apresentar dashboard situacional referente ao

tráfego processado contendo:

- a) Shadow IT: quantidade de aplicações descobertas e novas aplicações;
- b) Malware: Visão geral sobre os artefatos maliciosos encontrados;
- c) URLs: Domínios com maior registro de bloqueio pela ferramenta.

13.2.14. O referido painel deverá conter ainda capacidade de adicionar dashboards adicionais para fins de aumentar a visibilidade sobre o tráfego processado, contendo categorias como:

- a) Data loss prevention;
- b) Malware;
- c) Behavior Analytics;
- d) Dispositivos;
- e) Aplicações SaaS.

13.2.15. A solução deverá apresentar painel de comportamento para cada usuário do Ministério da Cultura, identificando credenciais vazadas na internet, bem como o histórico de registros que permita identificar atividades anormais do usuário.

13.2.16. O painel de malware deverá exibir informações relevantes para todos os incidentes relacionados a identificação de artefatos maliciosos, contendo informações que auxiliem na mitigação do evento de vazamento, apresentando as informações conforme segue:

- a) Severidade do malware identificado;
- b) Usuários envolvidos no incidente;
- c) Data e hora da detecção;
- d) Ação;
- e) Aplicação envolvida;
- f) Hash do arquivo identificado;
- g) Engine de malware que auxiliou na detecção;

13.2.17. A console única e centralizada de gestão deverá apresentar os logs de acesso, com no mínimo os seguintes campos:

- a) Usuário do Ministério da Cultura (MinC);
- b) Nome da estação de trabalho;
- c) Domínio acessado;
- d) Regra que processou o tráfego;
- e) Geolocalização do acesso de origem;
- f) Instância da aplicação SaaS;

13.2.18. A console deverá possuir, dentre suas características, solução de relatório com capacidade de apresentar as mais diversas dimensões, medidas e outros campos que se façam necessários para a construção de relatórios e dashboards analíticos atendendo no mínimo aos seguintes casos de uso:

- a) Relatório contendo a quantidade de malwares identificados;
- b) Gráfico de tendência com a quantidade de aplicações SaaS

acessadas em um determinado período e a quantidade comparada com um período anterior;

c) Relatório contendo a quantidade de alertas relacionado a vazamento de dados nas 5 aplicações SaaS mais acessadas;

d) Relatório contendo os 5 usuários com maior volume de acesso e as 5 aplicações mais acessadas para cada um deles;

e) Gráfico de tendência apresentando o tráfego permitido e bloqueado para um determinado período;

f) Relatório contendo as aplicações identificadas no Shadow IT que contenham vulnerabilidades;

g) Relatório contendo quantidade de alertas, por tipo e data;

h) Relatório contendo domínios/hostnames em que a inspeção do túnel TLS não ocorreu.

i) Relatório contendo domínios com erros de inspeção TLS;

j) Relatório de Shadow IT, contendo a quantidade de aplicações SaaS descobertas, o percentual de risco e a quantidade de aplicações SaaS corporativas e não corporativas;

k) Relatório contendo o acesso a plataformas de Inteligência Artificial, incluindo quais usuários acessaram, as plataformas acessadas, bem como as atividades registradas em cada uma delas;

l) Relatório contendo usuários do Ministério da Cultura que apresentam alto risco através da análise e correlação de múltiplos eventos, incluindo Análise comportamental, upload para aplicações SaaS não corporativas, acesso a sites maliciosos, malwares identificados e por fim o compartilhamento de credenciais.

m) Relatório do módulo de incidentes de DLP contendo Incidentes de DLP em aberto, políticas com a maior incidência de ocorrências, incidentes por aplicação, instância da aplicação SaaS e severidade relacionada ao incidente,

n) Relatório do módulo de DLP contendo mapa de relacionamento entre país de origem, política de prevenção contra vazamento de dados, aplicação SaaS e país de destino, usuários com maior ocorrência de violações de DLP apresentando a quantidade de alertas

o) .Relatório contendo os alertas de comportamento incluindo a aplicação envolvida e a regra que identificou a anormalidade.

p) Relatório contendo os alertas de malware, gráfico de tendência na identificação de malware, quantidade de alertas de malware, quantidade de alertas de sites maliciosos e por fim as categorias de malware bem como de sites maliciosos.

13.2.19. Monitorar a experiência dos usuários com destino aos serviços do Microsoft Office 365 através da medição de latência entre a estrutura de processamento de dados do fabricante e a aplicação do Microsoft Office 365;

13.2.20. Armazenamento dos metadados processados durante 90 dias e permitir o encaminhamento de informações dos alertas gerados para um SIEM de propriedade do Ministério da Cultura.

13.2.21. Deverá possuir integração com serviços de diretório Microsoft Active Directory e Microsoft Azure Active Directory atualmente instalados no Ministério

da Cultura.

13.2.22. A solução deverá possuir integração com o Microsoft Active Directory ou Microsoft Azure Active Directory, de propriedade do Ministério da Cultura, para utilizar uma única base de diretório para sincronização dos usuários administrativos, autenticação e privilégios de acesso.

13.2.23. A solução deverá apresentar painel de comportamento para cada usuário do Ministério da Cultura, identificando o score de risco, identificação de credenciais vazadas na internet, bem como o histórico de registros que permita identificar

13.2.24. Todas a plataforma de segurança deverá suportar geração de logs detalhados de acesso dos usuários Web, Aplicações Cloud, Bloqueios de Segurança e acessos ou bloqueio de aplicações privadas via ZTNA.

13.2.25. Deverá suportar os seguintes métodos de redirecionamento de tráfego para inspeção no datacenter do fabricante:

- a) Cliente do próprio fabricante instalado na estação de trabalho;
- b) Túnel seguro (Generic Routing Encapsulation - GRE ou IPSEC) através do dispositivo SD-WAN proposto neste termo de referência;
- c) Túnel seguro (GRE ou IPSEC) através do Next Generation Firewall a ser instalado no Datacenter do Ministério da Cultura;
- d) Proxy explícito configurado no browser da estação de trabalho via GPO;
- e) Proxy reverso integrado com o Microsoft Office 365.

### 13.3. **Acesso remoto seguro baseado no conceito Zero Trust Network Access e Secure Web Gateway:**

13.3.1. Deverá atuar como um roteador em nuvem, garantindo baixa latência e canal seguro, para aplicações privadas hospedadas no datacenter do Ministério da Cultura;

13.3.2. Por se tratar de uma solução Confiança Zero ela deverá habilitar uma arquitetura de privilégio mínimo, Zero Trust, definindo uma política de acesso granular para fornecer às pessoas certas no contexto certo, o acesso menos privilegiado aos aplicativos ou recursos e reduzir a superfície de ataque.

13.3.3. Será permitida a inclusão de um appliance físico ou virtual no Datacenter do Ministério da Cultura para a comunicação segura entre nuvem do fabricante e servidores internos.

13.3.3.1. O appliance físico ou virtual inserido no ambiente do Ministério da Cultura não deverá requerer um endereço IP público para habilitar o acesso remoto dos usuários para as aplicações dentro do datacenter do Ministério da Cultura.

13.3.4. A solução deverá possibilitar o acesso remoto seguro, baseado no conceito ZTNA, através dos seguintes métodos:

13.3.4.1. Cliente nativo do fabricante, com suporte aos sistemas Windows, MacOS e Linux;

13.3.4.2. Browser nativo do sistema operacional para aplicações HTTP/HTTPS;

13.3.5. A solução deverá fornecer acesso remoto a aplicações e recursos internos do Ministério da Cultura (MinC), com os seguintes requisitos de segurança:

- 13.3.5.1. Validação da identidade do usuário no Microsoft Active Directory;
- 13.3.5.2. Túnel seguro baseado em TLS;
- 13.3.5.3. Privilégio mínimo de acesso, garantindo o recurso apenas a aplicação ou a resolução de nome da aplicação autorizada;
- 13.3.5.4. Validação da postura da estação de trabalho;
- 13.3.6. Deve ser possível criar políticas de acesso utilizando:
  - 13.3.6.1. Usuário
  - 13.3.6.2. Grupos do Microsoft Active Directory;
  - 13.3.6.3. Organizational Unit (OU) do Microsoft Active Directory;
- 13.3.7. Os usuários remotos, não devem possuir visibilidade de aplicativos não autorizados. Os recursos não autorizados não devem apenas ser inacessíveis, mas também completamente invisíveis.
- 13.3.8. As aplicações disponíveis/publicadas deverão suportar os seguintes formatos: FQDN, IP ou domínio.
- 13.3.9. A solução deverá apresentar análise comportamental do usuário para identificar comportamentos anômalos como: Quantidade de downloads de arquivos sensíveis na aplicação web interna, Incidente com severidade alta mediante configuração
- 13.3.10. A solução deverá ser capaz de redirecionar, no mínimo, os seguintes protocolos de aplicações hospedadas no datacenter do Ministério da Cultura:
  - a) VOIP
  - b) HTTPS
  - c) RDP
  - d) SSH
  - e) Telnet
  - f) SQL
  - g) Oracle
- 13.3.11. A solução deverá tratar de maneira granular o timeout de autenticação do usuário. Essas políticas deverão ser configuradas de maneira global ou por grupo/usuário e deverá, ainda, ser aplicada por aplicação.
- 13.3.12. A solução deve trazer o monitoramento da atividade dos usuários, dando às equipes de TI uma maneira de monitorar e gerenciar facilmente todas as atividades de forma granular, entendendo qual usuário, quando, qual aplicação, qual política autorizou ou negou o acesso e status da postura
- 13.3.13. A solução deverá fornecer o acesso à aplicação apenas, não ao contexto de rede.
- 13.3.14. Deverá permitir o redirecionamento seguro para mais de 400 (quatrocentas) aplicações internas.
- 13.3.15. Deverá ser capaz de autorizar o acesso ou não a aplicações internas baseada no perfil da máquina.
- 13.3.16. Deverá ser capaz de continuamente solicitar ao usuário que autentique novamente antes de ter acesso às aplicações privadas;
- 13.3.17. O acesso deve ser dedicado e exclusivo a aplicação designada na

rede, não sendo permitido acesso irrestrito a um host ou a rede;

13.3.18. A solução de ZTNA deverá prover acesso seguro e controlado baseado nos protocolos TCP e UDP a aplicações privadas do Ministério da Cultura através de cliente do próprio fabricante instalado na máquina;

13.3.19. A solução deverá suportar aplicações legadas baseadas em arquitetura cliente - servidor, operadas sob protocolos TCP/UDP;

13.3.20. Para habilitar o trabalho remoto a solução deverá permitir ingressar a estação de trabalho remota de maneira e segura no domínio do Ministério da Cultura (MinC);

13.3.21. A solução deverá permitir o uso do Microsoft Auto-Pilot para provisionamento seguro da estação de trabalho do usuário remoto;

13.3.22. Deverá prover acesso a aplicações baseada nas seguintes aplicações:

- a) SSH - TCP Porta 22;
- b) HTTP - TCP Portas 80, 443 e customizadas;
- c) RDP - TCP 3389 e UDP 3389;
- d) SQL Server - TCP 1333, 1434 | UDP 1434;
- e) SMB - TCP 445;
- f) FTP - TCP 21.

13.3.23. O acesso seguro as aplicações definidas poderão ser restritas, no mínimo, para:

- a) Usuário Único;
- b) Múltiplos Usuários;
- c) Grupos de Usuário;
- d) Unidade Organizacional (OU).
- e) Para cada acesso, a política deverá prover múltiplas possibilidades de ações, dentre elas:
- f) Permissão;
- g) Bloqueio;

13.3.24. Deve ser possível determinar apenas o endereço IP e porta de acesso da aplicação sem a necessidade de determinar um segmento de rede interno que o usuário remoto terá acesso;

13.3.25. Ao se conectar remotamente na solução para acesso a uma aplicação interna, a máquina remota não deve ter acesso, nem ser atribuído em um segmento de rede interna como em um sistema de VPN tradicional;

13.3.25.1. Não serão aceitas soluções que utilizem túneis IPSec.

13.3.26. Deverá ser capaz de continuamente solicitar ao usuário que autentique novamente antes de ter acesso às aplicações privadas em um IdP externo.

13.3.27. A solução deverá suportar a importação de usuários a partir do Microsoft Active Directory instalado no Ministério da Cultura (MinC).

13.3.27.1. Caso não suporte autenticação via Active Directory, a contratada deverá prover IdP para autenticação.

- 13.3.28. A solução de segurança deverá suportar função Pre-Logon para plataformas Microsoft.
- 13.3.29. A solução deverá prover acesso a aplicações Web (HTTPS) sem a necessidade de instalação de agentes.
- 13.3.30. A solução deverá prover capacidade de avaliação contínua do endpoint para avaliação das validações de conformidade.
- 13.3.31. Deverá permitir o acesso diferenciado para um mesmo usuário conforme as seguintes condições:
- a) Máquinas em conformidade: A partir de uma máquina gerenciada, com pré-requisitos de segurança identificados, deve permitir o acesso à aplicação;
  - b) Máquinas não conformes: A partir de uma máquina gerenciada, uma estação que não atenda aos requisitos de segurança, deve bloquear o acesso à aplicação.
- 13.3.32. O painel de gestão centralizado deverá apresentar as estações com agente instalando identificando o usuário, id da máquina.
- 13.3.33. Deverá ser possível habilitar ou desabilitar o túnel de ztna via console para uma determinada estação de trabalho.
- 13.3.34. Para a funcionalidade de avaliação de postura a solução deverá verificar os seguintes:
- a) Validação da presença de antivírus
  - b) Validação de certificado cliente confiável
  - c) Validação de máquina no domínio
  - d) Validação de processo executando no dispositivo
  - e) Validação de presença de um arquivo
  - f) Validação de chave de registro Windows
  - g) Validação de versão mínima de Sistema Operacional
- 13.3.35. A solução proposta deverá interceptar requisições Web e para aplicações SaaS, garantindo o controle em tempo real das requisições, contextualização do acesso, visibilidade, identificação das instâncias corporativas saas do Ministério da Cultura (MinC) e proteção contra ameaças.
- 13.3.36. Suportar inspeção de SSL/TLS em 100% do tráfego Web, sem limites de volume de transações ou percentual inspecionado, em protocolos TLS 1.0, 1.1, 1.2 e 1.3
- 13.3.36.1. Possibilidade de criar regras granulares de exceção a inspeção SSL/TLS, com base categorias de URL, host e domínios de destino, usuário, grupo, departamento ou tipo de browsers
- 13.3.37. A solução de proxy em nuvem, deve oferecer controles de proteção de dados e de ameaças com visibilidade e controle granular das atividades em aplicações SaaS para os protocolos HTTP e HTTPS:
- 13.3.38. Deverá ser capaz de processar tráfego Web (HTTP/HTTPS) nas portas 80, 443 e em portas customizadas, a exemplo: 8443, 8080, 8081;
- 13.3.39. A solução deverá permitir a customização de alertas em português do Brasil em páginas de bloqueio apresentadas ao usuário.
- 13.3.40. A solução deve ser capaz de identificar e controlar aplicações

dinâmicas como: Skype, P2P e TOR browser

13.3.41. Deve ser possível a criação de políticas de filtragem de URL com base nos seguintes critérios:

- a) Categoria do site;
- b) Departamento ou OU, Grupo e usuário específico;
- c) Localidade da contratada ou IP de Origem;
- d) Protocolo: HTTP, HTTPS;
- e) Atividade: Browse, Upload, Download, Login, Logout
- f) Sistema Operacional, suportando a identificação de MacOS, Windows, Linux, IOS e Android

13.3.42. A solução deve permitir a definição de uma janela de tempo onde a regra deve valer. Exemplo: De 08AM até 18h PM;

13.3.43. A solução deve ser capaz de identificar via reconhecimento do tráfego web e não web e bloquear/liberar o uso de aplicações instaladas no desktop - a exemplo: Dropbox, Amazon Drive, SSH, RDP, Telnet, RealVNC, Teamviewer, dentre outras.

13.3.44. A solução deverá suportar a liberação de acesso ao canal do youtube do Ministério da Cultura (MinC) e de outros órgãos do governo (Exemplo: Canal do STF, Canal do STJ, Canal da PGR) e restrição aos demais canais e vídeos disponíveis, baseando-se em:

- a) Identificação nativa do ID do canal do youtube para liberação e bloqueio dos demais;
- b) Integração por meio da API do Youtube. O licenciamento da franquia de cotas do Youtube é de responsabilidade da CONTRATADA e deverá estar licenciado para no mínimo 1.000 cotas por usuário/mês;
- c) Dado a complexidade de liberação dos canais governamentais e de outras necessidades corporativas do Ministério da Cultura (MinC), não serão aceitas soluções que utilizem listas de URL e ID, devido a constante mudança imposta pelo youtube.

13.3.45. A solução deverá suportar a identificação da instância do Microsoft Office 365 do Ministério da Cultura (MinC), permitindo acesso a ele, porém restringindo acesso a suíte Microsoft Live (Outlook Live, Teams Live, OneDrive Live) e também restrição quanto a ações em outras instâncias do Microsoft Office 365.

13.3.46. Possuir categorização dinâmica de URLs de no mínimo para 100 categorias e serviço de reclassificação;

13.3.47. Permitir Criação de categorias customizadas para filtragem web, incluindo listas de bloqueio e de permissão;

13.3.48. Ao identificar uma aplicação SaaS, a solução deverá apresentar o risco da aplicação, incluindo a capacidade de identificar se a aplicação identificada possui algum registro de vazamento recente

13.3.49. Decodificar serviços SaaS corporativos e não corporativos, incluindo análise de risco do serviço SaaS:

- a) Visibilidade e controle do tráfego corporativo com direção ao Microsoft Office 365, em tempo real a partir de estações de trabalho gerenciadas e não-gerenciadas;



b) Visibilidade e controle em tempo real de acesso a URLs, por meio de classificação baseado em categorias;

13.3.50. A solução deverá estar licenciada e suportar os seguintes métodos para encaminhamento do tráfego para a solução de Proxy em nuvem:

a) Integração com o NGFW;

b) integração com WAF;

c) Proxy Explícito em nuvem;

d) Cliente nativo do próprio fabricante para no mínimo as plataformas Windows, MacOS, Linux, Aindroid e iOS.

13.3.51. Dentre as capacidades da solução para o entendimento do tráfego a ser inspecionado, deverá constar:

a) Base contendo, no mínimo, 100 categorias de URLs;

b) Deve ser capaz de identificar e controlar nativamente 40.000 aplicações SaaS;

c) Deve ser capaz de reconhecer o tráfego de rede para identificar mais de 400 aplicações;

d) Aplicar ação de bloqueio em tempo real para Microsoft Office 365, aplicações SaaS terceiras e Web;

13.3.52. A solução deverá oferecer controle e proteção para o acesso Web dos usuários, garantindo:

13.3.52.1. Controle de acesso a categorias não autorizadas.

a) Caso de Uso: A solução deverá prevenir o acesso a URLs associadas as categorias de Pornografia, Drogas, Atividades Criminais e Apostas.

13.3.52.2. Controle de acesso a categorias que impõem risco de segurança aos usuários do Ministério da Cultura.

a) Caso de Uso: A solução deverá prevenir o acesso a URLs associadas às categorias de Botnets, DGA, Command Control, Sites Maliciosos e Phishing.

b) Caso de Uso: A solução deve ser capaz de interceptar requisições de DNS e bloqueá-la com destino a domínios relacionados a Command & Control, Phishing, DGA, Botnet, Spam, Spyware e Malware.

13.3.52.3. Controle de acesso a categorias não categorizadas pelo fabricante:

a) Caso de Uso: A solução deverá prevenir o acesso a URLs não conhecidas pela base de inteligência do fabricante;

13.3.52.4. Permitir a criação de categorias customizadas baseadas em listas contendo regex ou domínios;

a) Caso de Uso: A solução deverá permitir o acesso em caráter de exceção a uma URL ou Domínio associado a uma categoria bloqueada.

13.3.53. A solução deverá permitir a criação de listas de exceção de tráfego que não devem ser encaminhadas à nuvem do fabricante:

a) Caso de Uso: A solução deverá permitir a conexão direta para categorias que incluem sites de Bancos e serviços financeiros;

13.3.54. Deve permitir a rastreabilidade do acesso via log para as exceções criadas.

- 13.3.55. A solução deverá permitir a configuração de quais categorias de URL e domínios que devam ter a inspeção do túnel TLS ativada.
- 13.3.56. A solução deverá permitir a configuração de quais aplicações SaaS que devam ter a inspeção do túnel TLS ativada.
- 13.3.57. O controle nativo de aplicações SaaS deverá apresentar visibilidade mínima sobre os seguintes contextos:
- a) Identificação do usuário e grupo;
  - b) Validação do dispositivo (gerenciado ou não gerenciado);
  - c) Categoria da aplicação SaaS;
  - d) Nível de risco da aplicação SaaS;
  - e) Geolocalização do usuário;
  - f) Controle granular de atividades (upload, post, edit, share, view, download, send).
- 13.3.58. Para aplicações Web 2.0 a solução deverá oferecer controles granulares, dentre eles:
- a) Facebook: Prevenir o vazamento de dados na ação de POST e bloquear as ações de POST, LIKE, SHARE e UPLOAD;
  - b) Youtube: bloquear as ações de DELETE, LIKE, SHARE, POST e VIEW para categorias de canais específicos;
  - c) Twitter: Prevenir o vazamento de dados nas ações POST e UPLOAD e ser capaz de bloquear as ações de POST, FOLLOW e DELETE;
  - d) Pastebin: Prevenir o vazamento de dados via ação POST e controlar ações de POST, DELETE e CREATE.
- 13.3.59. A solução deverá possibilitar a liberação de um período de hora por dia para acesso a Youtube e Mídias Sociais.
- 13.3.60. A solução deverá permitir, de maneira nativa, a criação de regras para permitir o acesso à plataforma do Office 365 Corporativo e negar o acesso às instâncias pessoais da Microsoft Live Suite (Exemplo: Hotmail, OneDrive Live, Outlook).
- 13.3.61. A solução deverá ser capaz de bloquear a ação de upload de arquivos para o Whatsapp Web.
- 13.3.62. A solução deverá permitir o upload/download de arquivos com destino a instância do Microsoft Office 365 do Ministério da Cultura e prevenção de upload e demais aplicações SaaS de Webmail e Cloud Storage.
- a) Caso de Uso - Office 365: Deve permitir as ações de upload e download com direção a instância do Ministério da Cultura no Microsoft Office 365 One Drive;
  - b) Caso de Uso - SaaS Cloud Storage: Deve bloquear a ação de upload e download para a categoria Cloud Storage;
  - c) Caso de Uso - Webmail: Deve bloquear a ação de upload para a categoria Webmail.
- 13.3.63. A solução deverá permitir o controle e visibilidade das informações encaminhadas via canais corporativos.
- a) Caso de uso - a solução deverá prover controles em tempo real de inspeção de mensagens enviados via Microsoft Teams, aplicando

controles prevenindo o envio de mensagens sensíveis ou contendo artefatos maliciosos.

b) Caso de uso - a solução deverá prover controle em tempo real contra a cópia de dados sensíveis ou malwares para o cliente do Microsoft One drive instalado na máquina.

13.3.64. A solução deverá ser capaz de aplicar controles granulares de ações para mais de 40.000 aplicações SaaS, corporativas ou terceiras, garantindo que o Ministério da Cultura tenha controle granular sobre as atividades desejadas para cada uma delas.

13.3.65. Deve minimamente suportar as seguintes aplicações corporativas:

a) Microsoft Office 365 (Microsoft OneDrive, Microsoft Sharepoint, Microsoft Word Online, Microsoft Outlook.com, Microsoft Exchange Online, Microsoft Teams, Microsoft Power BI).

b) Amazon AWS (S3, EC2, Cloud Trail, Cloud Watch, CodeBuild, CodeCommit, CodePipeline, Amazon Devops Guru, Amazon Drive, Amazon EKS, Amazon DynamoDB).

c) Microsoft Azure (Azure Admin, Azure Devops)

d) Google Workspace (Google Mail, Google Chat, Google Hangouts, Google Drive, Google Admin, Google API Console, Google Accounts, Google Biquery, Google Calendar)

e) Github e gitlab

13.3.66. Para as aplicações mencionadas no item 13.3.65 , desde que aplicável, a solução ser capaz de aplicar os controles listados abaixo:

- I - Create;
- II - Delete;
- III - Download;
- IV - Edit;
- V - Restore;
- VI - Send;
- VII - Upload;
- VIII - Move;
- IX - Reboot;
- X - Shutdown;
- XI - Attach;
- XII - Detach;
- XIII - Login;
- XIV - Logout;
- XV - Purchase;
- XVI - Start;
- XVII - Stop;
- XVIII - Terminate;
- XIX - Print.

13.3.67. Para aplicações SaaS desenvolvidas pelo Ministério da Cultura ou de desenvolvimento nacional, a solução deverá apresentar capacidade de customização de interpretador para registro de ações, a exemplo: Upload, Download, Search, dentre outros.

13.3.68. 1. 68. A solução deverá suportar capacidades de Firewall como serviço para os métodos de implantação com agentes instalados nas máquinas dos usuários, em todas as plataformas, e sem o uso de agentes no caso de implantação com túneis GRE ou IPSec

13.3.69. Toda a inspeção e aplicação de política de Firewall, independentemente do método de implantação, deverá ser realizada na nuvem.

13.3.70. A solução deverá suportar a criação de regras nos métodos utilizando túneis e agentes, com base em:

- a) Usuário do Microsoft Active Directory ou IDP próprio;
- b) Grupo do Microsoft Active Directory ou IDP Próprio;
- c) OU ou Departamento do Microsoft Active Directory ou IDP Próprio;

13.3.71. A solução deverá identificar no mínimo 300 aplicações como SSH, RDP, Banco de Dados, DNS sobre HTTPS, FTP, NFS, P2P BitTorrent, WhatsApp entre outras utilizando DPI (Deep Packet Inspection) independente se elas estão, ou não, utilizando portas padrões dos seus protocolos;

13.3.72. A solução deverá suportar a criação de políticas combinando todos as variáveis acima, como por exemplo criar uma regra específica para um grupo de usuários do IdP próprio ou Microsoft Active Directory, provenientes de uma Localidade específica, para bloqueio de uso da Aplicação SSH, independente da porta utilizada pelo servidor de SSH

13.3.73. A solução de FWaaS deverá possuir a capacidade de criar políticas específicas granulares para proteção de DNS;

13.3.74. A solução deverá ser capaz de interceptar e-mails encaminhados para domínios externos e identificar conteúdos sensíveis.

- a) Caso de uso - o envio de e-mails através do cliente Microsoft outlook (conexão via MAPI) instalado na estação de trabalho deverá ser inspecionado pela solução através de motores posicionados em nuvem.

13.3.75. A solução deverá ser capaz de interpretar o tráfego de rede e identificar aplicações não autorizadas como *Ultrasurf*.

13.3.76. A solução deverá suportar políticas para controle de resolução DNS, contendo:

- a) Usuário, grupo e OU ou Departamento do Microsoft Active Directory ou IDP próprio;
- b) Localidade de origem;
- c) Perfil DNS, contendo: Domínios autorizados, não autorizados e registros permitidos (A, NS, CNAME, SOA, PTR, MX, TXT, AAAA, SRV, CERT, ANY);
- d) Proteção contra riscos de segurança, como phishing, sites comprometidos, botnets, command control e domínios registrados recentemente.

13.3.77. A solução deverá suportar e bloquear tráfego DNS tunelado (VPN Over DNS, DNS over HTTP, DNS2TCP, IODINE);

- 13.3.78. Deve possuir detecção e proteção de malwares para:
- a) Todo tráfego Web de saída;
  - b) Inspeção dos seguintes protocolos: HTTP e HTTPS
  - c) Adwares, Backdoor, Dialer, Downloader, Criptografado, Exploit, Hacktool, Heuristic, Keylogger, Infostealer, Packed, Potentially unwanted applications, ransomware, rootkit, Spyware, Virus, Trojans e Worms
- 13.3.79. A solução deve possuir uma arquitetura de proxy (HTTP/HTTPS) de modo que todo o conteúdo de uma conexão seja analisado e inspecionado e após avaliação e veredito que uma nova conexão seja realizada para o destino final.
- 13.3.80. Deve fornecer proteção nativa para no mínimo:
- a) ActiveX vulneráveis;
  - b) Exploits de Browser;
  - c) URL's Maliciosas;
  - d) Proteção contra tráfego de Comando e controle;
  - e) Proteção contra servidores de Comando e controle;
  - f) Sites conhecidos de Phishing;
  - g) Sites suspeitos de Phishing através de IA;
  - h) Crypto Mining;
  - i) Spyware Callback;
  - j) Web Spam;
  - k) Sites conhecidos de Adware e Spyware;
  - l) Requisições de Cross-site Scripting;
  - m) Cookie Stealing;
  - n) Países proibidos;
  - o) Anonimizadores;
  - p) Proteção para tuneladores de tráfego: SSH Tunneling e IRC Tunneling;
  - q) Proteção nativa contra TOR;
  - r) Proteção nativa contra BitTorrent
  - s) Arquivos protegidos por senha; e
  - t) Arquivos que não possam ser escaneados.
- 13.3.81. A solução deverá prover capacidade de proteção dos usuários do Ministério da Cultura (MinC) contra malwares:
- a) Análise de artefatos por meio de assinaturas;
  - b) Análise de artefatos por meio de heurística;
  - c) Análise comportamental de artefatos Portable Executable via Sandbox.
  - d) Análise sem assinatura para identificação de malware;
  - e) Análise estática sem a execução do arquivo

- f) Análise do binário para identificar indicadores de atividade maliciosa;
- 13.3.82. O módulo de ameaça avançada deverá empregar modelos baseado em machine learning para identificar ameaças, anomalias e comportamento para arquivos portable executable, PDF, arquivos Microsoft Office e URLs maliciosas nos arquivos.
- 13.3.82.1. A solução deverá ser capaz de identificar um usuário que foi identificado com uma ameaça única entre todos os usuários do Ministério da Cultura (MinC).
- 13.3.82.2. A solução deverá utilizar técnicas avançadas baseadas em machine Learning para identificar situações de phishing.
- 13.3.83. A solução deverá possuir nativamente categorias relacionadas a risco de segurança, prevenindo contra:
- a) Phishing;
  - b) Domínios DGA;
  - c) Botnets
  - d) Sites comprometidos;
  - e) Servidores Command Control;
  - f) Spam;
  - g) Spyware;
  - h) Malware;
- 13.3.84. A solução deverá empregar capacidade de análise profunda do tráfego web por meio de solução de prevenção contra intrusão, prevenindo que estações de trabalho do Ministério da Cultura (MinC) sofram ataques a partir de sites comprometidos.
- 13.3.85. A solução deverá empregar controles robustos para identificação de ransomware, incluindo desde o monitoramento do comportamento do usuário ao tentar criptografar pastas do Microsoft One Drive Corporativo, como possuir engines que tratem este tipo de ameaça.
- 13.3.86. A solução deverá monitorar e bloquear quaisquer tentativas de acesso a artefatos do tipo ransomware a partir de plataformas SaaS não corporativas, porém legítimas, como por exemplo: Github, Amazon S3, Google Drive, Microsoft One Drive Live, dentre outras.
- 13.3.87. A solução deverá prover integração com o Microsoft Azure Active Directory para, ao identificar uma situação de risco, mover o usuário de grupo para que ele esteja contido em uma regra mais restritiva de acesso a Web.
- 13.3.88. A solução deverá prover integração com plataformas de EDR, XDR e SIEM para intercâmbio de IOC, utilizando padrões livres, como por exemplo STIX/TAXII.
- 13.3.89. A solução deverá empregar técnica de isolamento de Browser para domínios não categorizados, Anonymizers, Domínios registrados recentemente, dentre outros, prevenindo que os usuários do Ministério da Cultura (MinC) insiram informações no site ou até mesmo bloqueando downloads não solicitados.
- 13.3.90. A Solução deve possuir funcionalidade de monitoramento de experiência do usuário:

a) A solução deverá realizar monitoramento de latência a partir da máquina do usuário, passando pelo datacenter do fabricante com destino a aplicações corporativas SaaS (Microsoft Office 365).

b) Deve possuir informações detalhadas dos dispositivos: Sistema operacional, número de série do hardware, Plataforma (Sistema Operacional).

c) A solução deverá empregar testes contínuos de latência para medir o tempo entre o cliente e o datacenter e do data center até a aplicação Microsoft Office 365.

d) Os testes de medição de latência devem ocorrer independente da localização do cliente.

## **EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO**

**Portaria SPOA/MINC N° 142/2024 (1851460)**

**Ramon Leonn Victor  
Medeiros**

Integrante Técnico  
Assinado eletronicamente

**Franciana Von  
Wurmb**

Integrante Requisitante  
Assinado eletronicamente



Documento assinado eletronicamente por **Ramon Leonn Victor Medeiros, Integrante Técnico da Equipe de Planejamento da Contratação**, em 11/11/2024, às 15:59, conforme horário oficial de Brasília, com fundamento no art. 30, inciso II, da Portaria nº 26/2016, de 01/04/2016, do Ministério da Cultura, Publicada no Diário Oficial da União de 04/04/2016.



Documento assinado eletronicamente por **Franciana Von Wurmb, Fiscal de Contrato**, em 11/11/2024, às 16:07, conforme horário oficial de Brasília, com fundamento no art. 30, inciso II, da Portaria nº 26/2016, de 01/04/2016, do Ministério da Cultura, Publicada no Diário Oficial da União de 04/04/2016.



A autenticidade deste documento pode ser conferida no site [https://sei.cultura.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://sei.cultura.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **1967314** e o código CRC **96BA397B**.