



**MINISTÉRIO DA CULTURA**  
**SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E INOVAÇÃO**  
Esplanada dos Ministérios, Bloco B, - Bairro Zona Cívico Administrativa, Brasília/DF, CEP 70068-900  
Telefone: - <http://www.cultura.gov.br>

**CADERNO DE ESPECIFICAÇÕES TÉCNICAS**

**ANEXO I**

**PROCESSO: 01400.013362/2023-15**

**DOCUMENTOS  
RELACIONADOS**

**OBJETO** - Solução de prevenção contra vazamento de informações em meio digital (Data Loss Prevention - DLP) com fornecimento de licenças e ferramenta de descoberta e classificação de dados, controle de acesso, monitoramento de atividade, auditoria e proteção através de bloqueio, criptografia e quarentena, para aplicações e ambientes de armazenamento em nuvem, Cloud Access Security Broker (CASB), incluindo implantação da solução, treinamento e suporte técnico pelo período de 36 (trinta e seis) meses

ESTUDO TÉCNICO PRELIMINAR 73/2023

TERMO DE REFERÊNCIA 84/2023

CONTRATAÇÃO: 420001/90065/2023

**QUADRO DE COMPOSIÇÃO - GRUPO/LOTE E ITENS.**

LOTE	ITEM	DESCRIÇÃO
01	1	Aquisição de licenças de software de solução de prevenção contra vazamento de dados - Data Loss Prevention - DLP
	2	Configuração e Instalação
	3	Repasse de Conhecimento
02	4	Aquisição de licenças de software de solução de descoberta e classificação de dados, controle de acesso, monitoramento de atividade, auditoria e proteção através de bloqueio, criptografia e quarentena, para aplicações e ambientes de armazenamento em nuvem - CASB - Cloud Access Security Broker
	5	Configuração e Instalação
	6	Repasse de Conhecimento

1. **ITEM 01 - AQUISIÇÃO DE LICENÇAS DE SOFTWARE DE SOLUÇÃO DE PREVENÇÃO CONTRA VAZAMENTO DE DADOS - DATA LOSS PREVENTION - DLP**

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

## 1.1. Gerenciamento da solução de Prevenção de Perda de Dados

- 1.1.1. A solução deve fornecer uma estrutura de política única em todos os canais de exfiltração de dados (por exemplo, e-mail, Web, aplicativos SaaS, Impressão, aplicações, Mídia Removível, Compartilhamento de Arquivos);
- 1.1.2. Todas as funções de gerenciamento, incluindo alterações de configuração e upgrades, devem ser conduzidas a partir de um console central;
- 1.1.3. O sistema deve apoiar o acesso baseado em funções e a administração delegada com funções pré-definidas e personalizáveis:
  - Auditor
  - Gerente de Incidentes
  - Gerente de Políticas
  - Super Administrador
  - Administrador
- 1.1.4. A solução proposta deve oferecer suporte à integração com Active Directory ou File Directory (CSV);
- 1.1.5. A solução deve oferecer suporte à criação/exceção de política com base no diretório de usuário/grupo, máquina, rede, domínio;
- 1.1.6. A solução deve ter a capacidade de auditar alterações (por exemplo, logon/off, alterações de regras, logs do sistema, logs de tráfego);
- 1.1.7. Capacidade de o sistema notificar quando está tendo problemas de conexão;
- 1.1.8. Capacidade de integração (via syslog ou extração de banco de dados) com ferramentas de SIEM para fins de registro e alerta;
- 1.1.9. A solução deve fornecer escalabilidade futura para todos os componentes integrantes da arquitetura que compõe o sistema de DLP;
- 1.1.10. A solução deve oferecer suporte a ambientes de infraestrutura virtualizados, como Azure ou AWS para o portal de gerenciamento, banco de dados e outros componentes.
- 1.1.11. A solução deve ter integração nativa com Classificações de Dados (Baldon James, Microsoft AIP, Seclore, Titus).
- 1.1.12. A solução proposta deve ser capaz de implantar o agente usando métodos comuns de implantação de software, como GPO, SCCM, JAMF etc.
- 1.1.13. A solução deve fornecer a capacidade de verificar o status do agente e relatar quaisquer agentes que não estejam funcionando corretamente;
- 1.1.14. As comunicações com os módulos da solução e sistemas integrados devem ser criptografadas, via https (entrada/saída);
- 1.1.15. A solução deve oferecer suporte ao Microsoft RMS;
- 1.1.16. A solução deve usar um banco de dados relacional corporativo, como SQL;
- 1.1.17. O módulo de gerenciamento (servidor e console) deverá possuir compatibilidade para instalação, no mínimo, nos sistemas operacionais:
  - Windows Server 2008 R2 SP1;
  - Windows Server 2012;
  - Windows Server 2012 R2;
  - Windows Server 2016;
- 1.1.18. A arquitetura da solução deve oferecer suporte a sites remotos e usuários de rede distribuídos em muitos locais diferentes.
- 1.1.19. A solução deve descrever em meios de implantação típicos e onde cada componente reside.
- 1.1.20. A solução deve oferecer suporte à autenticação de dois fatores para acesso do administrador ao console de gerenciamento
- 1.1.21. A solução deve suportar os seguintes algoritmos de criptografia:
  - AES (128)
  - AES (256)

- Triple DES

- 1.1.22. A solução deve ter uma API RESTful disponível para incidentes de obtenção e atualização
- 1.1.23. Solução deve ser capaz de ser implantada em Máquinas Virtuais AWS EC2 e Azure
- 1.1.24.
- 1.1.25.

## 1.2. **Configuração de políticas de segurança de dados e detecção de conteúdo confidencial**

- 1.2.1. A solução deve ter políticas específicas de conformidade "prontas para uso" com base na região e no tipo de setor.
- 1.2.2. A solução deve ter políticas pré-definidas (1500+) baseadas em RegEX, Dicionários ou Scripts e deve ser capaz de selecionar políticas com base na correlação do país e das indústrias.
- 1.2.3. A solução deve fornecer políticas predefinidas para identificar possíveis expressões que sejam indicativas de cyberbullying, padrões autodestrutivos ou descontentamento dos funcionários
- 1.2.4. A solução deve ter políticas de Indicadores de Risco de Roubo de Dados (por exemplo, dados enviados em horários incomuns, e-mail para concorrentes, comunicação suspeita de malware, currículos etc.)
- 1.2.5. A solução deve ter a capacidade de usar uma única política para varrer os dados onde quer que sejam armazenados, transmitidos ou usados, tanto na rede quanto no terminal.
- 1.2.6. A solução deve permitir modificar os canais de destino podem para quaisquer políticas. (Ex: incluir em uma política utilizando o protocolo SMTP , poder incluir os protocolos HTTP e HTTPS.
- 1.2.7. Deve configurar exceções baseadas em regras de forma simples evitando geração de falsos positivos
- 1.2.8. A solução deve permitir uma sintaxe flexível para vincular dados a aplicativos específicos, servidores de arquivos, compartilhamentos de rede, impressoras e padrões de conteúdo exclusivos
- 1.2.9. A solução deve oferecer suporte a tipos de arquivo verdadeiros predefinidos
- 1.2.10. A solução deve oferecer suporte a condições de políticas com base na lógica booleana (AND, OR, NOT)
- 1.2.11. A solução deve suportar dados confidenciais em diferentes idiomas, incluindo mas não limitando o suporte para Português do Brasil e Inglês.
- 1.2.12. A solução deve extrair e inspecionar o conteúdo baseado em texto de arquivos e anexos;
- 1.2.13. A solução deve analisar os metadados do arquivo
- 1.2.14. A solução deve oferecer suporte a impressão digital de arquivo parcial e de hash completo para todos os canais de exfiltração de dados
- 1.2.15. A solução deve distinguir entre diferentes tipos de PII ou PHI. Ex: Distinguir entre os nove dígitos sociais de um cliente (CPF) e número de segurança de um número de telefone de nove dígitos sem a presença de uma palavra-chave
- 1.2.16. A solução deve suportar a inspeção de tipos de arquivos de arquivos (ZIP, TAR) para detectar o conteúdo com impressão digital.
- 1.2.17. A solução deve suportar a análise de arquivos e anexos grandes (20 MB e maiores) durante o processo de impressão digital do conteúdo.
- 1.2.18. A solução deve fornecer um método para dados de impressão digital, como registros de clientes (dados estruturados)
- 1.2.19. A solução deve proteger pelo menos 10 milhões de linhas de conteúdo específico de um banco de dados de informações confidenciais sem depender de palavras-chave ou padrões
- 1.2.20. A solução deve oferecer suporte a um método de detecção de aprendizado de máquina para códigos-fonte, formulários.
- 1.2.21. A solução deve suportar regras totalmente personalizáveis com expressões regulares, palavras-chave, frases-chave e dicionários

- 1.2.22. A solução deve oferecer suporte ao conteúdo da lista de permissões para remover com segurança a detecção de conteúdo textual
- 1.2.23. A solução deve oferecer suporte à detecção de várias palavras-chave com base em um peso especificado
- 1.2.24. A solução deve suportar pelo menos 5.000 listas de palavras-chave exclusivas
- 1.2.25. A solução deve suportar correspondência de padrões combinada com validação. Por exemplo, detectar padrões comuns de números de cartão de crédito como bem como fazer a validação da soma de verificação para garantir um número de cartão de crédito válido;
- 1.2.26. A solução deve detectar formatos de arquivo criptografados conhecidos e desconhecidos;
- 1.2.27. A solução deve identificar tags de rótulos de metadados de Boldon James, Proteção de Informações do Azure ou outras soluções de classificação de dados;

### 1.3. **Configuração de proteção para estações de trabalho**

- 1.3.1. O agente da solução deve ser compatível com MacOS e WindowOS
- 1.3.2. O agente da solução deve ser compatível com VMWare Horizon e Citrix XenApp
- 1.3.3. O agente da solução deve fornecer proteção contínua de dados confidenciais, independentemente de o usuário estar dentro ou fora da rede. A última política aplicada deverá ser sempre a política padrão
- 1.3.4. A solução deve detectar tentativas do usuário de enviar dados confidenciais por e-mail e Web (HTTP/S)
- 1.3.5. A solução deve impedir que os usuários enviem dados confidenciais por qualquer aplicativo no computador endpoint sem precisar abrir uma solicitação de recurso para oferecer suporte a novos aplicativos.
- 1.3.6. A solução deve impedir a exfiltração de dados por meio de mídia removível (por exemplo, unidades USB)
- 1.3.7. A solução deve ser capaz de aplicar políticas diferentes mesmo quando os usuários estão usando o mesmo endpoint
- 1.3.8. As tarefas de descoberta de dados de endpoint devem ter uma opção de agendamento:
  - uma vez;
  - diariamente;
  - semanalmente;
  - continuamente
- 1.3.9. A tarefa de descoberta de dados de endpoint deve ter configurações flexíveis para verificar apenas quando o computador estiver ocioso ou pausar a verificação enquanto o computador estiver funcionando com baterias
- 1.3.10. A tarefa de descoberta de dados deve oferecer suporte à inclusão e exclusão por tipo de arquivo, pastas, idade ou tamanho
- 1.3.11. A tarefa de descoberta de dados deve oferecer suporte a opções de varredura completas e diferenciais
- 1.3.12. A descoberta de dados deve ter uma opção para preservar o tempo de acesso original
- 1.3.13. O agente da solução deve aproveitar as tags de rótulos de metadados MIP ou Boldon James para impor a classificação ou reclassificar quando um arquivo violar uma política de dados em repouso
- 1.3.14. O agente precisa ser auto-regenerativo e resistente a adulterações.
- 1.3.15. Deve monitorar a área de transferência do sistema operacional e tomar medidas com base nos dados copiados e/ou protegidos.
- 1.3.16. A solução precisa oferecer suporte a opções de implantação de sistemas operacionais virtualizados.
- 1.3.17. O agente precisa oferecer uma mensagem pop-up que possa conter informações customizadas quando o usuário violar uma política
- 1.3.18. A mensagem pop-up deve fornecer uma oportunidade para fornecer justificativa comercial quando a política permitir esta ação.
- 1.3.19. A justificativa do usuário deve ser registrada/armazenada em um método que possa ser lido por outros sistemas"

- 1.3.20. Os arquivos copiados para dispositivos removíveis devem ser criptografados e o conteúdo deve ser legível apenas em ativos de propriedade da empresa
- 1.3.21. O agente deve oferecer suporte à visibilidade de dados copiados para dispositivos de mídia removível específicos
- 1.3.22. O agente da solução deve oferecer suporte à criptografia de nível de administrador e senha de auto criptografia para o usuário quando os arquivos são copiados para mídia removível
- 1.3.23. O agente de endpoint precisa ter o mínimo ou nenhum impacto no desempenho da máquina.
- 1.3.24. O agente da solução deve oferecer suporte a políticas hierárquicas de usuário/grupo com correção/resposta configuráveis.
- 1.3.25. O agente da solução deve ser compatível com os navegadores Edge Chromium, Firefox, Safari (Apple) e Chrome
- 1.3.26. O agente da solução deve oferecer suporte ao monitoramento e bloqueio de dados confidenciais carregados para aplicativos em nuvem não autorizados e armazenamento em nuvem
- 1.3.27. O agente da solução deve oferecer suporte a um processo para desabilitar o agente do endpoint com autorização
- 1.3.28. O agente da solução deve oferecer suporte à capacidade de confiar no aplicativo, configurando-o para não ser monitorado.
- 1.3.29. O agente da solução deve oferecer suporte às seguintes operações em dados confidenciais que podem ser executadas nas estações de trabalho:
- 1.3.30. Copiar e colar controles (ou seja, atividades da área de transferência)
- 1.3.31. Controle de impressão em impressoras locais ou de rede
- 1.3.32. Salvar conteúdo em diferentes locais, incluindo salvar em:
  - Pastas locais
  - Compartilhamentos de arquivos remotos
  - Unidades removíveis conectadas a um sistema de endpoint, como unidades USB
  - Salvar em locais de armazenamento em nuvem

#### 1.4. **Configuração de proteção para rede - Email**

- 1.4.1. A solução deve ser integrada ao Enterprise SMTP Gateway ou pode ser colocada entre um gateway SMTP corporativo para realizar a análise DLP
- 1.4.2. A solução deve dar suporte ao Exchange Online (no local, híbrido ou O365)
- 1.4.3. A solução deve ter capacidade de implantar gateways SMTP no Azure para se integrar facilmente ao O365
- 1.4.4. A solução deve oferecer suporte à quarentena de e-mail para e-mails que violaram as políticas de DLP
- 1.4.5. A solução deve ter criptografia nativa ou pelo menos integrar-se a ferramentas de criptografia de terceiros via X-Headers
- 1.4.6. A solução deve oferecer suporte a anexos de arquivo maiores que 25 MB para análise de DLP
- 1.4.7. A solução deve suportar quarentena, criptografar, descartar anexos e permitir ações de correção de e-mail
- 1.4.8. A solução deve oferecer suporte à análise de reconhecimento óptico de caracteres (OCR) com base nas políticas de DLP criadas

#### 1.5. **Configuração de proteção para rede – Web**

- 1.5.1. A solução fornece a capacidade de evitar vazamento de dados pelo canal SSL ao integrar com seu próprio gateway sem a necessidade de solução de terceiros ou dependência do protocolo ICAP
- 1.5.2. A solução deve monitorar vários tipos de tráfego na web: webmail, postagem na web e outros protocolos usando HTTP/S
- 1.5.3. A solução deve monitorar o tráfego FTP ativo e passivo
- 1.5.4. A solução deve bloquear e permitir ações de correção da Web

- 1.5.5. A solução deve oferecer suporte a by-pass quando ocorrer um erro inesperado
- 1.5.6. A solução deve suportar páginas de bloqueio personalizáveis
- 1.5.7. A solução deve ter a capacidade de monitorar portas/protocolos adicionais além de HTTP/HTTPS
- 1.5.8. A solução deve ter o Secure ICAP nativo para integração com Proxy, NGFW ou CASB
- 1.5.9. A solução deve suportar integração com outros proxies via ICAP ou encadeamento de proxy
- 1.5.10. A solução precisa dar suporte à implantação do Azure
- 1.5.11. A solução deve oferecer suporte à análise de reconhecimento óptico de caracteres (OCR) com base nas políticas de DLP criadas

**1.6. Configuração de proteção para rede - Monitoramento**

- 1.6.1. A solução deve suportar o modo de conexão SPAN/Mirror Port
- 1.6.2. A solução deve oferecer suporte a VLAN
- 1.6.3. A solução deve suportar a inclusão de redes específicas
- 1.6.4. A solução deve suportar a inclusão de serviços específicos (HTTP,Email,FTP) e portas
- 1.6.5. A solução deve oferecer suporte à análise de OCR com base nas políticas de DLP criadas

**1.7. Prevenção de Perda de Dados para Nuvem**

- 1.7.1. A solução deve aproveitar a mesma estrutura de política de outros canais DLP para canais DLP Cloud API e DLP Cloud Proxy (in-line)
- 1.7.2. A solução deve ter integração de API com os principais aplicativos em nuvem: Office365, G-Suite, Box, Dropbox, Salesforce e ServiceNow
- 1.7.3. A solução deve ter controle DLP granular para M365 Teams, OneDrive e SharePoint
- 1.7.4. A solução deve oferecer suporte à análise para atividades de upload, download e compartilhamento de aplicativos na nuvem para identificar possíveis violações de DLP
- 1.7.5. A solução deve oferecer suporte às seguintes ações de correção para análise de atividades de API: quarentena com nota personalizável, quarentena sem nota, cancelamento de compartilhamento externo, cancelamento de compartilhamento interno, cancelamento de compartilhamento de tudo e somente auditoria
- 1.7.6. A solução deve ser capaz de monitorar/controlar atividades de upload/download de aplicativos em nuvem que violem as políticas de DLP de dispositivos não gerenciados e gerenciados
- 1.7.7. A solução deve ter granularidade para aplicar políticas apenas para aplicativos de nuvem específicos com base na operação do usuário (por exemplo, upload/anexação/download de arquivos)
- 1.7.8. A solução deve oferecer suporte à varredura de dados em repouso por meio de conexão de API para Office365, G-Suite, Box, Dropbox, Salesforce e ServiceNow
- 1.7.9. A solução deve oferecer suporte a ações de correção para varredura de dados em repouso quando os arquivos violam políticas de DLP
- 1.7.10. A solução deve oferecer suporte às seguintes ações de correção para varredura de dados em repouso: quarentena com nota personalizável, quarentena sem nota, cancelar compartilhamento externo, descompartilhar interno, cancelar compartilhamento de tudo e auditar apenas
- 1.7.11. Capacidade de aplicar políticas granulares com base na atividade do usuário do aplicativo na nuvem (API offline): upload de arquivos, download de arquivos, compartilhamento de arquivos externos, compartilhamento de arquivos não reconhecidos)
- 1.7.12. Capacidade de aplicar políticas granulares com base na atividade do usuário do aplicativo na nuvem (Real-time-Inline): upload de arquivos, anexação de arquivos, download de arquivos
- 1.7.13. A solução deve ser capaz de aplicar políticas de dlp por aplicativos de nuvem

- 1.7.14. A solução deve ter capacidade de criar políticas de DLP com base em predicados diferentes, como localização, funcionalidade de aplicativos em nuvem, registro de dispositivo (gerenciado versus não gerenciado),
- 1.7.15. A solução deve ter a capacidade de aplicar políticas com base na pontuação de impacto nos negócios que consiste em uma regra básica de detecção com uma pontuação numérica, e essas pontuações são divididas em quatro níveis diferentes: Crítico, Alto, Médio e Baixo.
- 1.7.16. A solução deve oferecer suporte a aplicativos de nuvem personalizados em linha (HTTPS) sem a necessidade de abrir uma solicitação de recurso e também deve oferecer suporte à proteção DLP para upload/download
- 1.7.17. Capacidade de suportar qualquer aplicativo em nuvem inline (HTTPS) sem a necessidade de abrir uma solicitação de recurso com o fornecedor, e também deve suportar proteção DLP para upload/download
- 1.7.18. A solução deve ter diferentes tipos de modo de implantação: API, integração SSO via SAML 2.0 ou instalação do agente
- 1.7.19. A solução deve ter suporte para adicionar proxy reverso ao fazer a integração SSO via SAML 2.0
- 1.7.20. Capacidade de oferecer suporte à proteção sem agente ao acessar a partir de dispositivos não gerenciados
- 1.7.21. A solução deve fornecer análise de comportamento de risco do usuário com base nas atividades do usuário de aplicativos em nuvem
- 1.7.22. Capacidade de suportar regras de detecção de anomalias para aplicativos em nuvem: Força Bruta, tomada de conta, insider malicioso, comprometido e atividade suspeita por um usuário privilegiado.

## 1.8. **Configuração de proteção para Dados em Repouso**

- 1.8.1. A solução deve oferecer suporte à verificação de dados em repouso para Exchange, Outlook PST, bancos de dados, Sharepoint e sistemas de arquivos
- 1.8.2. A solução deve dar suporte ao OAuth 2.0 para verificação de dados em repouso do Exchange Online
- 1.8.3. A solução deve suportar SMB, NFS e CIFS para compartilhamentos de arquivos baseados em Windows e não Windows
- 1.8.4. A solução deve oferecer suporte aos métodos de verificação TCP ou ICMP ao pesquisar compartilhamentos de rede
- 1.8.5. As tarefas de descoberta de dados devem ter uma opção de agendamento: uma vez, diariamente, semanalmente ou continuamente
- 1.8.6. A tarefa de descoberta de dados deve oferecer suporte à inclusão e exclusão por tipo de arquivo, pastas, idade ou tamanho
- 1.8.7. A tarefa de descoberta de dados deve oferecer suporte a opções de varredura diferencial e completa
- 1.8.8. A descoberta de dados deve ter uma opção para preservar o tempo de acesso original
- 1.8.9. A descoberta de dados deve oferecer suporte à alocação de largura de banda para verificação do processo de descoberta
- 1.8.10. A descoberta de dados deve oferecer suporte aos recursos de reconhecimento óptico de caracteres (OCR)

## 1.9. **Gerenciamento de incidentes**

- 1.9.1. A solução deve fornecer a capacidade de escalar incidentes críticos para gerentes ou proprietários de dados
- 1.9.2. A solução deve fornecer controles de segurança e acesso em torno do caso/incidente (usuário e grupo)
- 1.9.3. A solução deve atribuir incidentes/casos a usuários de diferentes Unidades de Negócios
- 1.9.4. A solução deve permitir a definição e o estabelecimento de fluxos de trabalho específicos (ou seja, adicionar todos os três tipos de eventos aos casos), atribuir casos a usuários/proprietários individuais, permitir que os usuários adicionem notas etc.
- 1.9.5. A solução deve oferecer suporte ao monitoramento e gerenciamento de aspectos críticos e fases de cada incidente/caso e fases de cada incidente/caso até a resolução, envolvendo administradores autorizados especificados e usuários específicos da função, conforme necessário durante todo o processo
- 1.9.6. A solução deve fornecer a capacidade de mostrar apenas determinados incidentes de um departamento específico ao ponto focal atribuído desse departamento

- 1.9.7. A solução deve fornecer a capacidade de liberar automaticamente um e-mail em quarentena, postar a aprovação do gerente sem qualquer intervenção manual no console DLP
- 1.9.8. A solução deve oferecer suporte a scripts de correção para planos de ação de DLP (por exemplo, quando um arquivo viola as políticas de DLP, as soluções deixam um arquivo de exclusão com uma notificação)
- 1.9.9. A solução deve oferecer suporte ao Fluxo de Incidentes (Workflow) via API para liberar e-mails de quarentena

**1.10. Dados em repouso**

- 1.10.1. A solução deve oferecer suporte à varredura de dados em repouso para Exchange, Outlook PST, bancos de dados, Sharepoint e sistemas de arquivos
- 1.10.2. A solução deve oferecer suporte ao OAuth 2.0 para dados do Exchange Online na varredura em repouso
- 1.10.3. A solução deve oferecer suporte a SMB, NFS e CIFS para compartilhamentos de arquivos baseados em Windows e não Windows
- 1.10.4. A solução deve oferecer suporte a métodos de verificação TCP ou ICMP ao pesquisar compartilhamentos de rede
- 1.10.5. As tarefas de descoberta de dados devem ter uma opção de agendamento por: uma vez, diariamente, semanalmente ou continuamente
- 1.10.6. A tarefa de descoberta de dados deve oferecer suporte à inclusão e exclusão por tipo de arquivo, pastas, idade ou tamanho
- 1.10.7. A tarefa de descoberta de dados deve oferecer suporte a opções de varredura diferencial e completa
- 1.10.8. A descoberta de dados deve ter uma opção para preservar o tempo de acesso original
- 1.10.9. A descoberta de dados deve oferecer suporte à alocação de largura de banda para a varredura do processo de descoberta
- 1.10.10. A descoberta de dados deve oferecer suporte a recursos de Reconhecimento Óptico de Caracteres (OCR)

**1.11. Relatórios e Alertas**

- 1.11.1. A solução deve permitir a investigação de incidentes envolvendo dados em repouso, dados em uso e dados em movimento a partir de um console de gerenciamento centralizado.
- 1.11.2. A solução deve fornecer resumo e agrupamento de relatórios personalizados em diferentes variáveis e atributos.
- 1.11.3. A solução deve suportar exportações de relatórios de incidentes via planilha, XML, PDF ou HTML.
- 1.11.4. A solução deve ter relatórios pré-definidos para auxiliar nas investigações.
- 1.11.5. A solução deve suportar a capacidade de salvar relatórios personalizados e filtros de incidentes.
- 1.11.6. A solução deve suportar a capacidade de definir permissões de relatórios por departamentos.
- 1.11.7. A solução deve usar análise de dados avançada para fornecer à sua equipe de operações de segurança um relatório de classificação de pilha sobre os principais riscos de segurança de dados em sua organização
- 1.11.8. A solução deve ser capaz de gerar relatórios programados
- 1.11.9. A solução deve fornecer relatórios flexíveis de incidentes (diário, semanal, mensal, trimestral etc.)
- 1.11.10. A solução deve ser capaz de relatar o número de alertas gerados por destino
- 1.11.11. A solução deve permitir que os usuários criem mensagens de alerta personalizáveis para administradores, usuários e gerentes de usuários
- 1.11.12. A solução deve fornecer um catálogo de relatórios abrangente que forneça um "drill-down" para facilitar a investigação dos incidentes de maior risco
- 1.11.13. A solução deve ser capaz de fornecer dados forenses dentro do mesmo registro de incidente.
- 1.11.14. A solução deve priorizar instantaneamente casos de níveis de risco alto a baixo com limites de pontuação de risco personalizáveis fornecidos em uma pilha de relatórios de classificação de risco de incidente
- 1.11.15. A solução deve capturar dados de eventos com metadados apropriados (data/hora, usuário, protocolo)



- 1.11.16. A solução deve suportar um protocolo de cadeia de custódia
- 1.11.17. A solução deve reter os logs por pelo menos um ano, se não for possível, a solução deve oferecer suporte ao arquivamento de incidentes
- 1.11.18. A solução deve ter a capacidade de alterar a gravidade:

- Alta;
- Média;
- Baixa

- 1.11.19. A solução deve ter a capacidade de alterar seu o status:

- Novo;
- Em Processo;
- Fechado;
- Falso Positivo;
- Escalado;

## 1.12. **Módulo de Classificação de Informação**

- 1.12.1. A solução deverá possuir engine de classificação baseado em Inteligencia Artificial.
- 1.12.2. O produto deve ter seu autoaprendizado alimentado por um sistema de machine learning.
- 1.12.3. A solução deverá integrar-se de forma automatica com soluções de DLP.
- 1.12.4. O software deverá suportar de forma automatica as principais normas ( ECC-2018, GDPR, PII, ISSO 27001, PCI, CMMC, SAMA, NCA etc.
- 1.12.5. Para funcionamento da solução, caso seja necessário uso de banco de dados, todo licenciamento da solução deve ser de responsabilidade da contratada.
- 1.12.6. Deverá recomendar níveis de conformidade e classificação ao usuário usando Inteligência Artificial, Machine Learning e tentativas de log para expor ou desclassificar a informação.
- 1.12.7. A solução deverá funcionar tanto on premises quanto em nuvem.
- 1.12.8. O produto deverá gerar e agendar automaticamente os relatórios.

### i. Aplicação de Classificação

- Deverá ter a capacidade de escolher mais de um valor de classificação (múltiplas seleções).
- Deve permitir funcionalidade de exibir aos usuários a solicitação de classificar documentos por uma caixa de diálogo pop-up.
- A solução deve permitir a rotulagem assistida, orientando o usuário através de escolhas de classificação para garantir seleções válidas.
- Deve possuir opções de classificação marcadas dinamicamente para esquemas avançados (como ITAR, CUI, SAMA, PII etc.).
- Deve possuir a capacidade de ter uma classificação padrão ou classificação sugerida pela solução.
- A solução deverá solicitar ao usuário para classificar documentos ao salvar, imprimir ou enviar um e-mail.
- A solução deverá aplicar tag em imagens e suporte a vídeo por meio do clique com o botão direito do mouse no Windows Explorer.
- O produto deverá aplicar tag em arquivos CAD por meio do clique com o botão direito do mouse no Windows Explorer.
- A solução deverá aplicar tag (etiquetas) em MS Visio e o Project por meio do clique com o botão direito do mouse no Windows Explorer.
- Deve ter a capacidade de criar expressões regulares (Regexes) para sugestões de classificação no painel do produto.
- A solução deve possuir regras de rotulagem padrão (automáticas) para o Agente. Como por exemplo, permitir que todos os arquivos e e-mails novos ou modificados serão classificados por padrão, ou seja, Internos ou Confidenciais.
- Capacidade de configurar regras de rotulagem padrão (automáticas) e individualmente por plug-in compatível no mínimo com Microsoft Word, Microsoft Excel, Microsoft Power Point e Microsoft Outlook.
- O agente deve se atualizar automaticamente.
- A solução deve possuir autenticação com LDAP para os agentes instalados nas estações de trabalho dos usuários.

- Deve possibilitar a classificação em massa de arquivos com um clique com o botão direito do mouse pelo Windows Explorer.

## ii. Funcionalidade do Agente para MacOS

- Deve possuir etiquetas exclusivas e não exclusivas para utilização de no mínimo:
  - i. Tags de classificação;
  - ii. Tags de conformidade;
  - iii. Tags de atributos e quaisquer outras etiquetas personalizadas.
- Possuir capacidade de adicionar vários cabeçalhos flutuantes ao mesmo documento (ou seja, um cabeçalho para interno e um cabeçalho para conformidade de PCI).
- A solução deve ter a capacidade de configurar a aparência visual para cabeçalho e rodapé individualmente nos documentos classificados.

## iii. Requisitos Gerais de Políticas

- A solução deve oferecer suporte a classificação automatizada, sugerida e orientada pelo usuário.
- A solução deve avaliar o conteúdo, contexto, identidade e outros atributos de dados não estruturados para tomar decisões de classificação e política.
- A solução deve ter um mecanismo de política simples e flexível para apoiar a criação de regras. Por exemplo, possuir granularidade que permita o bloqueio de envio de e-mails confidenciais, mas permitir criar exceções por endereço de e-mail ou domínio de destino.
- A solução deve acionar ações de política e classificação com base em diferentes eventos, como Abrir, Salvar, Imprimir, Encaminhar, Fechar, Enviar ou Alteração de Classificação.
- A solução deve permitir que os administradores definam políticas com ou sem classificação como parte da política.
- A solução deve permitir que os administradores combinem políticas para fornecer um controle mais refinado.
- A solução deve suportar aninhamento/hierarquia de políticas para controlar o fluxo de execução de políticas, facilitando a manutenção de casos de uso mais avançados para classificação e aplicação de políticas.
- A solução deve fornecer ajuda contextual em toda a interface do usuário para oferecer suporte ao treinamento de segurança e ajudar os usuários a selecionarem as opções corretas de classificação e correção de política.

### 1.12.9. **Requisitos de classificação e identificação dos dados.**

- i. A solução deve suportar a classificação de mensagens e tarefas no Microsoft Outlook 2013/2016/2019 (ou versão superior) e no Exchange online.
- ii. A solução deve permitir a classificação de documentos do Microsoft Word, Microsoft Excel e Microsoft PowerPoint de todas as versões do Microsoft Office, desde o Office 2013 ao Office 365.
- iii. Deve fornecer um esquema de classificação consistente entre os aplicativos.
- iv. A solução deve suportar a capacidade de impor a classificação de e-mail (Microsoft Outlook, OWA e Office 365) e documentos, independentemente das extensões e tipos de arquivo.
- v. Deve suportar a capacidade de classificar em Enviar, Salvar/Salvar como, Imprimir, Novo e-mail, Fechar/Abrir documento e outros eventos de e-mail e documento.
- vi. O produto deve oferecer suporte a retenção de dados e tags, incluindo campos de dados para períodos de retenção
- vii. Deve exibir com destaque os valores de classificação (facilmente visíveis) no Microsoft Office, Microsoft Outlook e Office 365.
- viii. A solução deve reconhecer a classificação dos emails recebidos e exibir a classificação no Outlook.
- ix. A solução deve suportar diferentes valores de classificação para várias aplicações. Isso pode ser combinado com o direcionamento do usuário para apresentar opções de classificação detalhadas com base no aplicativo e na identidade do usuário.
- x. Permitir que os usuários atribuam valores de classificação por meio de uma interface de usuário de classificação de um clique.
- xi. A solução deve permitir que os usuários atribuam valores de classificação ao usar o recurso de resposta em linha do Microsoft Outlook 2013, 2016 e 2019 (ou superior).
- xii. O produto deve permitir que os usuários atribuam valores de classificação a qualquer tipo de arquivo clicando com o botão direito do mouse no Explorador de Arquivos e selecionando um ou mais arquivos.
- xiii. A solução deve dar suporte à população dinâmica de campos de classificação de fontes diferentes do esquema de classificação pré-configurado, inserindo vários atributos de metadados. Por exemplo, os valores de metadados podem vir de atributos de documentos (por exemplo, autor), variáveis ambientais e Active Directory (por exemplo, grupo, departamento).
- xiv. A solução deve oferecer suporte à solicitação de usuários para confirmar um valor de classificação automatizado (também chamado de "classificação sugerida").

- xv. Deve oferecer suporte à capacidade de solicitar que os usuários alterem a(s) classificação(ões) padrão se o padrão for inadequado para o conteúdo, contexto ou outros atributos do email ou documento.
- xvi. A solução deve oferecer suporte à capacidade de solicitar que os usuários classifiquem em alguns casos e usem a classificação automatizada em outros. Por exemplo, uma classificação padrão pode ser usada para email interno, mas os usuários são solicitados a classificar para email externo. Ou os usuários podem ser solicitados a classificar o email somente quando houver um anexo.
- xvii. Deve suportar a capacidade de verificar determinadas palavras-chave e expressões regulares e definir a classificação de acordo.
- xviii. Deve gerar metadados para todos os tipos de arquivos, incluindo metadados persistentes e incorporados para muitos arquivos que não são do escritório, ou seja, outras extensões/formatos, incluindo PDF, Visio, Project, imagens e arquivos de vídeo
- xix. Oferecer suporte à criação de metadados personalizados ilimitados para interoperabilidade (Departamento, tipo de PII, categoria de documento, contagem de PII etc.), incluindo custom X-headers.
- xx. A solução deve oferecer suporte a marcações visuais personalizáveis em e-mails e documentos (por exemplo, fonte(nome/tamanho/recursos), tamanho, cor e conteúdo).
- xxi. Deve suportar marcações visuais personalizáveis em Microsoft Outlook.
- xxii. A solução deve suportar a adição de marcações visuais na parte superior e inferior de um email.
- xxiii. A solução deve oferecer suporte à capacidade de adicionar marcas d'água em aplicativos suportados do Microsoft Office.
- xxiv. Deve oferecer suporte ao uso de variáveis em marcações visuais, tornando mais fácil para os administradores oferecer suporte a vários casos de uso em uma política.
- xxv. A solução deve suportar diferentes marcações visuais para a mesma classificação, dependendo do contexto. Por exemplo, um documento "Confidencial" com uma palavra-chave específica pode ter marcações diferentes de um documento "Confidencial" com PII.

#### **1.12.10. Requisitos de Relatórios e Auditoria**

- i. A solução deve registrar a atividade do usuário enquanto os usuários manipulam e-mails, documentos e arquivos.
- ii. Deve fornecer relatórios integrados.
- iii. A solução deve fornecer um conjunto inicial pré-construído de relatórios para o banco de dados de relatórios (em valores separados por tabulação/formato Excel ou Banco de dados).
- iv. Os valores de classificação no e-mail devem ser consistentes, independentemente do usuário acessar os e-mails das plataformas desktop, laptop
- v. Deve ter a capacidade de reter as classificações existentes nos encadeamentos de e-mails.

#### **1.12.11. Requisitos de configuração e gerenciamento**

- i. A solução deve fornecer um Console de Administração centralizado e baseado na Web para configuração de classificação e gerenciamento de políticas.
- ii. Deve oferecer suporte à configuração de implantação de um servidor central.
- iii. A console centralizada deve funcionar com base em um único agente no cliente das estações de trabalho.
- iv. A solução deve permitir que os clientes recuperem sua configuração de um servidor de gerenciamento central por meio de uma conexão segura (SSL/TLS).
- v. Deve permitir que os administradores enviem as configurações do cliente para os desktops dos usuários por meio do Servidor Central
- vi. A solução deve armazenar em cache as configurações localmente para uso offline.
- vii. Deve permitir que os agentes recebam as atualizações de política sem reiniciar os aplicativos do Microsoft Outlook e do Office.
- viii. A solução deve fornecer a capacidade de implantação em modo silencioso para que o software possa ser implantado e habilitado em diferentes fases.
- ix. Deve permitir que os administradores personalizem todas as cadeias de texto da interface do usuário para oferecer suporte a diferentes idiomas e terminologia. Isso inclui campos e valores de classificação e mensagens de aviso de política.
- x. A solução deve ser capaz de identificar informações como identidade, números de passaporte e informações de cartão de crédito para classificação automatizada por meio de recursos embutidos ou deve ter a capacidade de definir expressões regulares.
- xi. Ser compatível com Microsoft Office 2013 (32 bits e 64 bits), 2016, 2019 ou posterior.
- xii. Ser compatível com Windows 7, 8, 1 e 10 ou superior.

#### **1.12.12. Requisitos de integração e interoperabilidade**

- i. A solução deve suportar
  - Soluções DRM
  - Soluções DLP

- i. A solução deve fornecer a capacidade de anexar metadados a objetos de informação, alavancados por soluções de e-discovery.
- ii. Deve fornecer a capacidade de anexar metadados a objetos de informação, que podem ser aproveitados por soluções de prevenção de perda de dados (DLP) de terceiros e devem funcionar mesmo quando e-mails e documentos estiverem protegidos.
- iii. A solução deve fornecer a capacidade de gravar tags que a solução DLP possa ler.
- iv. Ter a capacidade de acionar a criptografia com base em metadados.
- v. A impressão deve ser controlada com base na classificação e no contexto
- vi. Permitir que o usuário aplique a classificação em massa em vários arquivos selecionados nas exibições do explorador de arquivos do Windows

#### 1.12.13. **Aplicação de marcações de classificação em Arquivos**

- i. Deve permitir as seguintes possibilidades de marcações:
- ii. Aplicar uma marcação ao cabeçalho de um arquivo
- iii. Aplicar uma marcação ao rodapé de um arquivo
- iv. Aplicar uma marca d'água a um arquivo
- v. Aplicar uma marcação de código de campo a um arquivo
- vi. Aplicar metadados persistentes a um arquivo
- vii. As marcações visíveis podem ser personalizadas, para que não afetem os modelos, o conteúdo existente, a estrutura ou a marca.

#### 1.12.14. **Classificação para Email**

- i. A classificação deve ser aplicada em Microsoft Outlook
- ii. Quando um e-mail é classificado, os destinatários e o remetente deverão ser verificados automaticamente no envio, para garantir que sejam apropriados - por exemplo, para evitar que um e-mail marcado como 'interno' vá para um domínio externo.
- iii. O nível de classificação de um email é atualizado automaticamente para corresponder ao nível de qualquer anexo (ou corresponder ao nível mais alto de classificação se houver mais de um anexo).
- iv. Os anexos podem ser verificados para garantir que estão classificados e a classificação não tenha expirado.
- v. A classificação pode verificar quantos destinatários estão no email
- vi. A classificação deve permanecer em um email mesmo na resposta de um destinatário externo
- vii. Deve aplicar marcações na primeira linha do texto
- viii. Deve aplicar marcações na última linha de texto
- ix. Deve aplicar marcações no assunto de um e-mail como prefixo ou anexado
- x. Deve aplicar marcações no cabeçalho de um email
- xi. Deve aplicar Gerenciamento de Direitos (por exemplo, Azure RMS, Seclore, Sealpath)
- xii. Deverá manter a classificação automática de e-mail externo para e-mail de entrada com base na última classificação de e-mail enviada pelo usuário interno.

#### 1.12.15. **Ações inteligentes de classificação.**

- i. Não permitir o usuário salvar ou imprimir sem classificar o documento.
- ii. Deve interromper a disseminação acidental de e-mail para usuários sem um nível de autorização apropriado.
- iii. Deve sugerir ou exigir uma classificação padrão com base na posição da empresa, departamento, localização, conteúdo do arquivo.
- iv. Possuir classificação obrigatória de um arquivo criado externamente ao ser aberto, compartilhado ou impresso.
- v. Deve detectar arquivos aninhados em um arquivo ou o corpo de um e-mail.
- vi. Deve detectar conteúdo em arquivos e sugerir ou exigir classificação.
- vii. Deve detectar conteúdo em arquivos aninhados e sugerir ou exigir classificação.

#### 1.12.16. **Proteção de modificação de Metadados**

- i. Todos os metadados devem ser persistentes, ou seja, os metadados removidos são reaplicados quando o arquivo é salvo, impresso ou enviado por e-mail.
- ii. Os usuários devem ser impedidos de alterar a classificação.
- iii. Os detalhes do usuário que classificou o arquivo devem ser registrados.

iv. Se um usuário tiver permissão para alterar a classificação, essa alteração deverá ser registrada.

#### 1.12.17. Gerenciamento de Políticas

- i. Possuir uma ferramenta de gerenciamento simples, onde as políticas podem ser criadas e modificadas
- ii. As regras de políticas devem ser criadas e editadas com um assistente simples.
- iii. As políticas podem ser personalizadas com uma ampla variedade de atributos - por exemplo, atributos do Active Directory.
- iv. Não deve possuir limite para o número de políticas que podem ser criadas.
- v. Deve possuir níveis de classificação ilimitados para permitir que uma política evolua.
- vi. A classificação pode ser alterada ao longo do tempo, à medida que as necessidades de negócios se desenvolvem.
- vii. As políticas devem se alinhar com as políticas internas de marcação e aplicação de uma empresa.
- viii. Deve permitir que uma variedade de elementos de classificação pode ser aplicada - por exemplo. seletores únicos, seletores múltiplos
- ix. Deve permitir que as políticas sejam facilmente testadas (modo de teste) antes da implantação .
- x. Deve permitir que a classificação seja obrigatória para o usuário.
- xi. As políticas devem permitir serem adaptadas para diferentes departamentos ou hierarquia - por exemplo, somente gerentes podem fazer downgrade de uma classificação.
- xii. As regras devem permitir serem adaptadas para diferentes departamentos ou hierarquia - por exemplo, as marcações visíveis não aparecem em um arquivo quando ele é impresso se o usuário estiver no Marketing.
- xiii. Deve permitir que os menus de classificação possam ser adaptados para diferentes departamentos ou hierarquia.
- xiv. Os botões de classificação devem ser agrupados (empilhados) em colunas (para que não ocupem muito espaço na faixa de opções).
- xv. Deve possuir suporte ao idioma Português Brasileiro.
- xvi. O suporte a idiomas deve ser automatizado com base na localização do usuário.

#### 1.12.18. Auditoria

- i. Todas as ações de classificação deverão ser registradas.
- ii. Deve possuir relatórios automatizados.

## 2. ITEM 04 - AQUISIÇÃO DE LICENÇAS DE SOFTWARE DE SOLUÇÃO DE DESCOBERTA E CLASSIFICAÇÃO DE DADOS, CONTROLE DE ACESSO, MONITORAMENTO DE ATIVIDADE, AUDITORIA E PROTEÇÃO ATRAVÉS DE BLOQUEIO, CRIPTOGRAFIA E QUARENTENA, PARA APLICAÇÕES E AMBIENTES DE ARMAZENAMENTO EM NUVEM - CASB - CLOUD ACCESS SECURITY BROKER

### 2.1. Arquitetura

- 2.1.1. A solução deve ter um único console para todas as funções de CASB;
- 2.1.2. A solução deve possuir agente único para estações de trabalho Windows e MacOS;
- 2.1.3. A solução deve oferecer suporte a qualquer aplicativo HTTP(S) de qualquer dispositivo sem um agente;
- 2.1.4. A solução deve comprovar 99,99% de disponibilidade do datacenter em nuvem.
- 2.1.5. A solução deve suportar mais de 300 PoPs (pontos de presença) espalhados pelo planeta para prover baixa latência de acesso;
- 2.1.6. A solução deve oferecer suporte ao Controle de Acesso Contextual;

### 2.2. Conformidade e Certificações

- 2.2.1. A solução deve ter certificação SOC-2 Tipo 2;
- 2.2.2. A solução deve ter as certificações ISO27001, ISO27017 e ISO27018;
- 2.2.3. Solução deve ter certificação FedRamp;
- 2.2.4. A solução deve ter um status em tempo real do serviço;

### 2.3. **Integrações**

- 2.3.1. A solução deve ter suporte a túneis IPSec;
- 2.3.2. A solução deve ter suporte a túnel GRE universal;
- 2.3.3. A solução deve possuir datacenters redundantes;
- 2.3.4. A solução deve oferecer suporte à integração com qualquer IdP compatível com SAML;
- 2.3.5. A solução deve oferecer suporte ao Agente de Sincronização do Active Directory.
- 2.3.6. Suporta o envio de dados de ameaças para um SIEM através de syslog;
- 2.3.7. A solução deve ter capacidade de exportação de logs para soluções de SIEM;
- 2.3.8. A solução deve ser integrada aos provedores de identidade para direcionar o tráfego por meio de proxy reverso após a autenticação;
- 2.3.9. A solução deve oferecer suporte para integração com soluções MDM/EMM para compilar uma lista de identificadores exclusivos de dispositivo;

### 2.4. **Registro em log e alertas**

- 2.4.1. A solução deve oferecer suporte à filtragem de violações com base em vários contextos, por exemplo: usuário, política, padrão de dados, intervalo de datas, etc.);
- 2.4.2. A solução deve oferecer suporte à classificação de violações com base em títulos da coluna (por exemplo, gravidade, política, status, data, etc.);
- 2.4.3. A solução deve fornecer o número de violações detectadas no documento ou objeto, usuário e a atividade;
- 2.4.4. A solução deve fornecer trechos do documento que desencadearam a violação com conteúdo correspondente realçado;
- 2.4.5. A solução deve suportar a marcação de violações com um status (por exemplo, falso positivo, novo, aberto, resolvido);

### 2.5. **Monitoramento histórico e em tempo real**

- 2.5.1. A solução deve oferecer suporte à capacidade de filtrar com base no tipo de atividade ou nas últimas semanas/dias;
- 2.5.2. A solução deve suportar a capacidade de digitar parâmetros de filtragem em uma barra de pesquisa/filtro para exibir atividades específicas, usuários, etc.
- 2.5.3. A solução deve oferecer suporte a atividades de filtragem com base em um intervalo de datas específico ou até 30 dias anteriores;
- 2.5.4. A solução deve permitir a visualização da postura de segurança e a exposição de risco para acompanhamento do impacto de segurança dos investimentos em cloud com os seguintes requisitos:
  - i. Visibilidade do Retorno de Investimento com relação as violações de dados evitadas;
  - ii. Score Card de segurança mostrando a utilização geral da plataforma de segurança, incluindo a adoção pelo usuário;
  - iii. Volume de dados confidenciais acessados por canal;
  - iv. Visão de Ameaças (malware);

### 2.6. **Administração**

- 2.6.1. A solução deve oferecer suporte a MFA para acesso ao Portal de Administração;
- 2.6.2. A solução deve oferecer suporte ao RBAC (Controle de Acesso Baseado em Função);
- 2.6.3. A solução deve oferecer suporte a uma função de administrador para criar e editar políticas;
- 2.6.4. A solução deve oferecer suporte a uma função de administrador específica para configurar novos aplicativos SaaS suportados, criar novos usuários e visualização dos alertas;
- 2.6.5. A solução deve oferecer suporte a diferentes modos de exibição personalizados para grupos de usuários e dashboards/relatórios específicos;

### 2.7. **Gestão de Identidades**

- 2.7.1. A solução deve oferecer suporte à funcionalidade nativa de logon único;
- 2.7.2. A solução deve oferecer suporte a recursos de IdP/IAM de entrada no caso de não haver nenhuma solução IDP/IAM disponível;
- 2.7.3. A solução deve oferecer suporte à autenticação multifator para aplicativos em nuvem como um mecanismo de mitigação de risco;
- 2.7.4. A solução deve oferecer suporte à integração com o Active Directory e o Azure AD para autenticação de usuário e sincronização de grupo de segurança e OU (Organization Unit);
- 2.7.5. A solução deve oferecer suporte à integração via SAML 2.0 com qualquer solução de gerenciamento de identidade para autenticar o acesso a serviços de nuvem sancionados;

2.8. **Notificações**

- 2.8.1. A solução deve oferecer suporte ao envio de um email para o usuário final quando uma política é acionada;
- 2.8.2. A solução deve oferecer suporte ao envio de um email para um administrador quando uma política é acionada.;
- 2.8.3. A solução deve oferecer suporte à criação de um incidente/alerta quando uma política é acionada;

2.9. **Controle de acesso contextual**

- 2.9.1. A solução deve oferecer suporte à permissão de políticas acesso específicas para dispositivos gerenciados;
- 2.9.2. A solução deve permitir o bloqueio de acesso a aplicações SaaS utilizadas/sancionadas pelo órgão quando a origem for de dispositivos não gerenciados;
- 2.9.3. Solução deve oferecer suporte ao bloqueio de acesso a aplicativos não sancionados;
- 2.9.4. Deve suportar políticas baseadas em departamento, geolocalização, dispositivo e Sistema Operacional e Navegadores (utilizando cabeçalho HTTP User-Agent);
- 2.9.5. Permitir que dispositivos pessoais visualizem conteúdo online, mas não baixem ou carreguem arquivos de aplicações SaaS;
- 2.9.6. A solução deve oferecer suporte à identificação de dispositivos gerenciados usando um agente;
- 2.9.7. A solução deve oferecer suporte à identificação de dispositivo gerenciado por um certificado de cliente;
- 2.9.8. A solução deve oferecer suporte à identificação de dispositivo gerenciado por um atributo SAML;
- 2.9.9. A solução deve suportar aplicar um adiamento do login do usuário, baseado em seu comportamento e risco, esse período deve ser configurado pelo administrador via política;
- 2.9.10. A solução deve oferecer suporte à configuração de um tempo limite ocioso personalizado, antes de impor a nova autenticação;
- 2.9.11. A solução deve oferecer suporte ao acionamento de MFA com base em grupo, dispositivo, localização, comportamento, intervalo de tempo ou qualquer combinação de critérios;

2.10. **Logs**

- 2.10.1. Deve suportar filtragem de violações com base em várias informações, por exemplo: usuário, política, tipo de detecção, intervalo de datas, etc.
- 2.10.2. A solução deve suportar a classificação de violações com base em cabeçalhos de coluna, por exemplo: gravidade, política, status, data, etc.
- 2.10.3. Deve fornecer o quantitativo de violações encontradas em documentos, objetos, usuários e na atividades;

2.11. **Análise e Controle de Geolocalização**

- 2.11.1. A Solução deve suportar detecção e bloqueio de logins de países não autorizados;
- 2.11.2. A solução deve suportar a detecção de logins simultâneos de locais geograficamente distantes, permitindo impor um fator adicional de autenticação, quando esse tipo de comportamento ocorrer;
- 2.11.3. A solução deve oferecer suporte à criação de locais personalizados para identificar sites e localidades remotas reconhecidas pelo órgão;

2.12. **Forense**

- 2.12.1. A solução deve oferecer suporte à capacidade de filtrar a trilha de auditoria de um usuário especificado para o período de tempo em torno do incidente;
- 2.12.2. A solução deve oferecer suporte à capacidade de exibir um feed de atividade para um usuário especificado;

2.13. **Funcionalidades de CASB para aplicações SaaS**

- 2.13.1. Suporte a realizar proxy inline de aplicativos SaaS
- 2.13.2. A solução deve oferecer suporte ao acesso inline a qualquer aplicativo HTTP(S) de qualquer dispositivo sem a necessidade de um agente instalado no dispositivo do usuário;
- 2.13.3. A solução deve oferecer suporte à configuração pré-definida para uso e integração com o Microsoft 365;
- 2.13.4. A solução deve oferecer suporte à configuração pré-definida para uso e integração com o Google Workspace;
- 2.13.5. A solução deve oferecer suporte à configuração pré-definida para uso e integração com o Salesforce;
- 2.13.6. A solução deve oferecer suporte à configuração pronta para uso do DropBox;
- 2.13.7. A solução deve oferecer suporte à configuração pronta para uso para Box.com;
- 2.13.8. A solução deve oferecer suporte à configuração pronta para uso do ServiceNow;
- 2.13.9. A solução deve oferecer suporte à configuração pronta para uso do Slack;
- 2.13.10. A solução deve oferecer suporte à configuração pronta para uso para a Atlassian;
- 2.13.11. A solução deve oferecer suporte à configuração pronta para uso para a AWS;
- 2.13.12. Deve suportar o bloqueio de acesso a aplicativos não sancionados;

2.14. **Prevenção de Ameaças Avançadas**

- 2.14.1. A solução deve oferecer suporte à detecção de malware hospedado em serviços de nuvem;
- 2.14.2. A solução deve suportar o monitoramento de dados armazenados em aplicativos em nuvem e detectar se há malware presente nos arquivos;
- 2.14.3. A solução deve suportar a varredura de armazenamento de dados em nuvem em busca de novas assinaturas / variantes de malware;
- 2.14.4. A solução deve oferecer suporte à funcionalidade de detecção avançada de ameaças integrada ao CASB;
- 2.14.5. A solução deve oferecer suporte para detectar e colocar em quarentena malwares de dia zero presente em serviços de nuvem;
- 2.14.6. A solução deve oferecer suporte a mais de um mecanismo de Antimalware;

2.15. **Integrações com Aplicações SaaS via API**

- 2.15.1. A solução deve oferecer suporte à varredura de todos os arquivos e pastas armazenados em aplicativos SaaS e detectar violações de políticas de DLP especificadas;
- 2.15.2. A solução deve oferecer suporte à exclusão de uma lista especificada de usuários de uma varredura;
- 2.15.3. A solução deve oferecer suporte ao direcionamento de uma varredura para uma lista especificada de usuários;
- 2.15.4. A solução deve oferecer suporte à varredura somente de novos arquivos e pastas adicionados ao Microsoft Onedrive desde a última verificação executada;
- 2.15.5. A solução deve oferecer suporte à varredura apenas de novos arquivos e pastas adicionados ao Google Drive desde a última varredura executada;
- 2.15.6. A solução deve oferecer suporte à quarentena de um arquivo que violou uma política de DLP em um aplicativo SaaS;
- 2.15.7. A solução deve oferecer suporte ao fornecimento de uma lista de todos os arquivos atualmente em quarentena com base em políticas;
- 2.15.8. Deve registrar e monitorar aplicativos SaaS via API;
- 2.15.9. A solução deve suportar uma ação de correção manual pelo administrador, permitindo por exemplo, liberar um arquivo que estava em quarentena.



2.15.10. A solução deve suportar a marcação de violações com um status, por exemplo: falso positivo, novo, aberto e resolvido;

2.15.11. A solução deve oferecer suporte a um painel interativo mostrando violações de DLP em aplicativos de nuvem;

2.15.12. A solução deve oferecer suporte para identificar todos os arquivos e categorizá-los automaticamente;

**2.16. Shadow IT**

2.16.1. A solução deve oferecer suporte à detecção e exibição de "Shadow IT" descobrindo uma gama completa de aplicativos de nuvem em uso.

2.16.2. A solução deve oferecer suporte à descoberta e classificação automáticas de centenas de milhares de aplicativos de nuvem não sancionados

2.16.3. A solução deve suportar a análise de logs de firewall/proxy de terceiros para gerar um relatório sobre todos os aplicativos ShadowIT que estão sendo usados em seu ambiente;

2.16.4. A solução deve oferecer suporte ao resumo do número agregado de serviços de nuvem em uso e do número de serviços de alto risco em uso;

2.16.5. A solução deve oferecer suporte à filtragem por categoria de serviço de nuvem, nível de risco, tipo de dispositivo, país, departamento e outros atributos;

2.16.6. A solução deve oferecer suporte à listagem de todos os usuários de cada serviço de nuvem com base em seu respectivo nome baseado no Active Directory;

2.16.7. Deve possuir, no mínimo, 24 (vinte e quatro) portas 10/100/1000 BaseT full-duplex ativas simultaneamente, autosense com conectores RJ-45 diretamente conectada ao chassi, sem conversores externos, com MDI/MDIX automático.

**3. ITENS 02 e 05 - CONFIGURAÇÃO E INSTALAÇÃO**

3.1. A solução de TIC deverá ser plenamente implementada pela Contratada no ambiente do MinC nas quantidades solicitadas em no máximo 60 (sessenta) dias corridos, a partir da assinatura da Ordem de Fornecimento ou Ordem de Serviço.

3.2. A empresa que realizar a implantação deverá ter técnicos treinados em toda a solução ofertada. Os serviços deverão ser prestados por técnicos devidamente capacitados, certificados pela fabricante da solução a qual deverá atuar quanto a implementação e demais procedimentos relacionados a configuração e implementação de políticas e demais requisitos exigidos.

3.3. Os serviços que eventualmente acarretem risco para os sistemas em produção ou requeiram parada de servidores, equipamentos e rede elétrica, somente poderão ser executados fora de expediente, em horários previamente acordados com a área de TI do local de instalação;

3.4. Caberá à Contratada o irrestrito cumprimento das seguintes prerrogativas:

i. Responsabilizar-se pela completa implantação do projeto, ou seja, todos os custos necessários à operacionalização dos equipamentos;

ii. Responsabilizar-se por todos os instrumentais necessários durante o período de implantação e testes de aceitação;

iii. Instalar e configurar todos os produtos do fornecimento da solução;

iv. Executar a integração de todos os produtos da solução, de modo a não prejudicar as atividades mantidas nos locais, podendo ser exigida a realização de algumas fases em horários noturnos e fins de semana para que seja cumprido o cronograma de entrega;

v. Elaborar a "Documentação e Finalização do Projeto", que consiste na consolidação de toda a documentação gerada no projeto, seja esta técnica e/ou gerencial.

**4. ITENS 03 e 06 - REPASSE DE CONHECIMENTO**

4.1. A CONTRATADA deverá repassar à CONTRATANTE todas as informações solicitadas e documentação da solução, além de disponibilizar treinamento conforme especificações a serem fornecidas no Termo de Referência.

4.2. O treinamento será demandado à CONTRATADA pela CONTRATANTE após a efetiva implementação e estruturação da solução de segurança em seu parque tecnológico, quando acordarão o cronograma para realização do treinamento.

4.3. O treinamento deverá ser em Brasília – DF, para a equipe técnica do CONTRATANTE.

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

- 4.5. O treinamento deverá 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.
- 4.6. Deverá ser ofertada para 1 (uma) turma com no máximo 10 alunos e com carga horária mínima de 40 (quarenta) horas.
- 4.7. Deverá ser fornecido certificado de conclusão emitido pelo fabricante.
- 4.8. Os horários do curso deverão seguir a conveniência do CONTRATANTE, podendo sua realização ocorrer apenas em um dos períodos do dia (manhã ou tarde).
- 4.9. Deverá ser fornecido material didático completo e com conteúdo oficial do fabricante.



Documento assinado eletronicamente por **Ramon Leonn Victor Medeiros, Integrante Técnico da Equipe de Planejamento da Contratação**, em 27/12/2023, às 16:16, 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 **1562329** e o código CRC **3A2E15FB**.