



**MINISTÉRIO DA SAÚDE**  
**FUNDAÇÃO NACIONAL DE SAÚDE**  
**COORDENAÇÃO DE INOVAÇÃO E INFRAESTRUTURA TECNOLÓGICA**  
**Setor de Autarquias Sul (SAUS) – Quadra 4 – Bloco N**  
**Brasília - CEP 70070-040**  
**(61) 3314-6619**

## **ANEXO I ESPECIFICAÇÕES TÉCNICAS**

### **1. Descrição da Solução de Tecnologia da Informação**

<b>ITEM</b>	<b>ESPECIFICAÇÕES TÉCNICAS E REQUISITOS MÍNIMOS</b>
1	Aquisição de licenças de software de solução de prevenção contra vazamento de dados - Data Loss Prevention - DLP
2	Treinamento

**1.1.** Este Anexo especifica as características técnicas da solução de Data Loss Prevention / DLP a ser adquirida para implementação no ambiente do FUNASA. Detalhamos neste Anexo os componentes da solução de DLP.

### **2. Plataforma Gerenciamento**

**2.1.** Deve ter console de gerenciamento via tecnologia Web (HTTP ou HTTPS).

**2.2.** O módulo de gerenciamento (servidor e console) deverá possuir compatibilidade para instalação, no mínimo, nos sistemas operacionais:

- 2.2.1.** CentOS;
- 2.2.2.** Debian;
- 2.2.3.** Ubuntu;
- 2.2.4.** Red Hat Enterprise Linux;
- 2.2.5.** Unix;
- 2.2.6.** Solaris;
- 2.2.7.** FreeBSD;
- 2.2.8.** Windows Server 2019.

**2.3.** O licenciamento da solução proposta deve contemplar todo o software, ou seja, todas as funcionalidades descritas neste edital.

**2.4.** As configurações de todos os módulos devem possuir integração nativa com a console central.

**2.5.** Suportar funcionamento em sistemas de virtualização.

- 2.6. A solução deve possuir ou integrar com sistemas de monitoramento de atividades do usuário baseado na nuvem (UAM), usando indicadores comportamentais (IOB) e fornecendo visibilidade significativa sobre comportamentos de risco do usuário, a fim de automatizar as políticas de proteção de dados em nível de usuário.
- 2.7. Capacidade de excluir incidentes em lote para gestão eficiente de espaço utilizado pela base de dados.
- 2.8. Suportar funcionamento em plataformas de Single Sign-On (SSO).
- 2.9. A solução deverá criptografar toda a comunicação que ocorre entre os servidores de gerenciamento e os agentes instalados em terminais.
- 2.10. A solução deverá criptografar a comunicação entre o servidor principal e os servidores adicionais da plataforma.
- 2.11. Possuir registros detalhados de auditoria de atividades de sistema.
- 2.12. Permitir a instalação em Sistema Operacional restrito, com serviços e configurações de porta limitados (Hardening).
- 2.13. Deve ter a capacidade de bloquear o acesso, movimentação, tráfego e cópia de informações confidenciais detectadas.
- 2.14. Deve possuir módulos de detecção distintos, para:
- 2.14.1. Localizar dados confidenciais armazenados em servidores de arquivos, bancos de dados e servidores de email;
  - 2.14.2. Localizar dados confidenciais armazenados em desktops e laptops;
  - 2.14.3. Detectar dados confidenciais em trânsito na rede, em protocolos TCP/IP;
  - 2.14.4. Detectar vazamento de dados a partir de conexão direta com servidores de email;
  - 2.14.5. Detectar vazamento de dados a partir de conexão direta com appliances responsáveis pelo processamento de tráfego WEB (Proxy ou UTM).
- 2.15. Capacidade de obter a “impressão digital” de dados estruturados e não estruturados.
- 2.16. Capacidade de normalizar variações comuns de apresentação de dados para aprimorar a precisão de políticas de monitoramento.
- 2.17. Capacidade de identificar dados estruturados e não estruturados, sem necessidade de utilização de servidores adicionais ou dedicados para este fim.
- 2.18. Detectar documentos não estruturados, após usar capacidades nativas de aprendizado automático, a partir da análise de um conjunto de amostras.
- 2.19. Permite a criação de padrão de identificação utilizando dados internos da instituição de modo a customizar a ferramenta.
- 2.20. Permitir detecção de acordo com expressões regulares configuráveis.
- 2.21. Permitir detecção por tipo de arquivo, por nome e extensão de arquivo, remetente/destinatário e protocolo de transmissão.
- 2.22. Capacidade de integrar diretamente com LDAP (MS Active Directory) para criar regras de detecção de terminal baseadas em usuário ou grupo. Políticas diferentes podem ser aplicadas de acordo com o usuário que fez o login, mesmo em uma máquina compartilhada.
- 2.23. Possuir mecanismo de envio de notificações personalizadas por e-mail aos administradores.
- 2.24. Permitir a criação de perfis para administração de servidores, administração de usuário, criação e edição de política.
- 2.25. Armazenar e exibir a mensagem original ou arquivo que gerou o incidente.

- 2.26. Exibir todo o histórico do incidente, inclusive as alterações e edições referentes ao mesmo.
- 2.27. Permitir a exportação da lista de incidentes no formato HTML, PDF ou CSV.
- 2.28. Interface de administração única para vizualização de todos os incidentes.
- 2.29. Possuir interface WEB, compatível, no mínimo, com os navegadores Internet Explorer, Mozilla Firefox e Google Chrome.
- 2.30. Permitir a configuração de ações automáticas, dependendo da quantidade de dados expostos.
- 2.31. Deve possuir integração com LDAP, para obtenção de detalhes e informações adicionais dos usuários envolvidos num incidente detectado.
- 2.32. Deve possuir integração com Active Directory, para autenticação de usuários da solução.
- 2.33. Deve possuir logs detalhados de auditoria de alterações de políticas.
- 2.34. A solução deve ter capacidade de descoberta de vazamento de dados nos seguintes canais:
  - 2.34.1. Nuvem;
  - 2.34.2. Email;
  - 2.34.3. Web;
  - 2.34.4. Terminais;
  - 2.34.5. Smartphones (A partir de um APP a ser instalado);
- 2.35. Plataforma de armazenamento de dados.
- 2.36. Proteger os dados contra exposição ou roubo em tempo real.
- 2.37. Deve suportar a verificação de arquivos compactados recursivos (exemplos .zip, .rar dentro de .zip, .rar).
- 2.38. Deve suportar de forma comprovada a detecção de dados no idioma português brasileiro.
- 2.39. Deve ter a capacidade de analisar conteúdo de arquivos grandes (maiores que 20MB) anexados em e-mails.
- 2.40. Deve identificar informações confidenciais sem a necessidade de acrescentar tags, etiquetas e afins nos arquivos de origem.
- 2.41. Deve identificar conteúdos armazenados em colunas específicas de planilhas eletrônicas e em bancos de dados.
- 2.42. Deve possuir capacidade para identificar conteúdos específicos com base em um padrão pré-determinado, para no mínimo:
  - 2.42.1. CPF;
  - 2.42.2. CNPJ;
  - 2.42.3. Cartões de Crédito;
  - 2.42.4. Número de eleitor;
  - 2.42.5. RG;
  - 2.42.6. IBAN;
  - 2.42.7. Dados de tecnologia com o IP Address, Mac Address e IMEI de telefones.
- 2.43. Deve detectar o arquivo pelo seu conteúdo real, e não apenas pela extensão do arquivo.
- 2.44. A solução deve possuir integrada na console a funcionalidade de workflow (Condições de acionamento) resposta a incidentes.
- 2.45. Devem ser exibidas na console de gerenciamento todas as informações a respeito do incidente para, no mínimo:

- 2.45.1. Dados para análise como: Origem, Destino, detalhes de qual Canal de detecção foi acionado e nome/caminho do arquivo;
- 2.45.2. Dados de qual regra foi acionada;
- 2.45.3. Dados de qual informação acionou a regra;
- 2.45.4. Severidade do incidente;
- 2.45.5. Status do incidente;
- 2.45.6. Nome da aplicação;
- 2.45.7. Data e hora do evento;
- 2.45.8. Volume de dados trafegados no incidente;
- 2.45.9. Nome do usuário referenciado no incidente;
- 2.45.10. Atributos do usuário coletados do Active Directory;
- 2.45.11. Nome da estação de trabalho;
- 2.45.12. Informações de destino para qual o dado seria copiado;
- 2.45.13. Histórico completo de alteração de incidentes.

2.46. Deve ter a capacidade de importar um conjunto de pré-configurações do sistema otimizadas para verticais das indústrias específicas, contando com dados de pesquisa em português.

2.47. A solução deve possuir, com mais de 1700 modelos de políticas predefinidos agrupados por localização geográfica e tipo de organização para identificar regras, regulamentos ou leis que a organização deve cumprir e aplicar as políticas correspondentes sem a necessidade de impressão digital dos dados envolvidos.

2.48. Deve possibilitar a realização de backup e restore de configurações, incidentes e políticas da plataforma.

2.49. Deve possibilitar integração nativa com soluções de classificação da informação, de forma a monitorar o uso de dados classificados nos canais de detecção e também a possibilidade de imposição de classificação durante a descoberta de dados em servidores de arquivos, por exemplo.

2.50. A solução deve ser agnóstica a linguística. Todos os mecanismos de identificação de dados, por exemplo: palavras, dicionários e Machine Learning, devem funcionar de forma igual em qualquer linguagem.

2.51. A solução deve proteger documentos em pelo menos 40 tipos de idiomas.

2.52. A solução deve incluir um mecanismo de análise de segurança, que é exclusivamente responsável pela modelagem estatística de dados e análise de comportamento suspeito dos usuários, com o objetivo de identificar e agrupar incidentes comuns a um determinado usuário ou estação de trabalho, automaticamente e usando uma pontuação de risco atribuída.

2.53. Deve permitir que sejam visualizados e identificados rapidamente os usuários ou estações de trabalho com o mais alto nível de risco para a organização, como resultado dos incidentes de segurança associados a eles.

### 3. Políticas e Detecção

3.1. Deve ter a capacidade de utilizar, no mínimo, os critérios abaixo para criação de políticas:

- 3.1.1. Palavra ou conjunto de palavras chave;
- 3.1.2. Identificadores pré existentes ou customizados (CPF, CNPJ, Cartão de crédito, etc.);
- 3.1.3. Expressões regulares com possibilidade de adaptação para o padrão de dados existentes;
- 3.1.4. Nível de classificação da informação;

- 3.1.5. Tipo de arquivo;
- 3.1.6. Nome e extensão de arquivos;
- 3.1.7. Bases de indexação previamente carregadas;
- 3.1.8. Tamanho de dados trafegados;
- 3.1.9. Quantidade de anexos de um e-mail;
- 3.1.10. Protocolos de rede ou canais da estação;
- 3.1.11. E-mails em dispositivos móveis;
- 3.1.12. Dados enviados para impressora;
- 3.1.13. Usuários/E-mails internos;
- 3.1.14. Estações de trabalho/servidores específicos;
- 3.1.15. Localização da estação de trabalho (Dentro ou fora da rede interna);
- 3.1.16. Tipo de estação (Laptop ou desktop);
- 3.1.17. E-mails ou domínios externos;
- 3.1.18. Direção do tráfego (Entrada ou saída);
- 3.1.19. Qualquer aplicação em execução na estação de trabalho;
- 3.1.20. Cópias para caminhos de rede.

3.2. A solução deve incluir mecanismos de proteção de dados contra vazamentos lentos e sofisticados (DRIP DLP), ou seja, deve monitorar a perda lenta de dados em eventos cumulativos;

3.3. A solução deve fornecer políticas predefinidas para identificar expressões potenciais que são indicativas de bullying cibernético, padrões de pensamento suicida ou conteúdo malicioso;

3.4. A solução deve ter inteligência artificial composta de técnicas que permitem aprender com exemplos de dados em vez de regras de dados pré-classificadas. O produto deve trabalhar com algoritmos de aprendizagem supervisionados e algoritmos de aprendizagem não-Supervisionados para classificar e aprender com as informações descobertas nos endpoints;

3.5. Deve possibilitar criação de regras de exclusões para as políticas de acordo com grupos de usuários fornecidos pelo active directory.

3.6. O produto deve possuir modelos de políticas de detecção com base em regulamentações e melhores práticas de mercado, para no mínimo:

- 3.6.1. SOX;
- 3.6.2. PCI;
- 3.6.3. HIPAA;
- 3.6.4. GDPR.

3.7. A solução deve possibilitar a criação de regras para adequação a LGPD.

3.8. A solução deve possuir templates de políticas de detecção, para no mínimo os seguintes temas:

- 3.8.1. Imagens com conteúdo inapropriado;
- 3.8.2. Linguagem ofensiva ou racismo;
- 3.8.3. Cyber Bullying;
- 3.8.4. Problemas relacionados a jogos de azar;
- 3.8.5. Dados confidenciais e propriedade intelectual;
- 3.8.6. Dados que envolvem segurança de redes;

- 3.8.7. Busca de informações relacionadas a indicadores de comprometimento.
- 3.9. Deve ter a capacidade para análise de conteúdo nos mais diversos tipos de arquivos, para no mínimo:
- 3.9.1. Texto (TXT, ASC, HTML, DOC, DOCX, SWX, ODT);
  - 3.9.2. Compactados (ZIP, RAR, GZ, LHA, HQX, JAR, 7z);
  - 3.9.3. CAD (DWG, DXF, VSD, DGN);
  - 3.9.4. Planilhas (XLS, XLSX, 123, SXC, ODS, CSV);
  - 3.9.5. Apresentações (PPT, PPTX, SXI, SXP, ODP);
  - 3.9.6. Outros (PDF, MDB).
- 3.10. Deve permitir criar políticas que combinam várias tecnologias e regras de detecção com regras "E/OU" lógicas e de exceção.
- 3.11. Permitir a escrita de expressões lógicas para configuração das regras de detecção, exemplo:("Condição 1" OU "Condição 2") E NÃO "Condição 3".
- 3.12. Deve ter a capacidade de construir políticas de detecção, configurando-se o grau de severidade adotado para cada regra criada, conforme o número de correspondências que se deseja encontrar em cada possível violação.
- 3.13. A solução deve fornecer a implantação de políticas DLP corporativas de forma unificada, ou seja, uma única política de DLP pode ser aplicada a todos os módulos (network, endpoints e aplicações em cloud).
- 3.14. As políticas de detecção devem possuir, no mínimo:
- 3.14.1. A capacidade de normalização de todas as variações comuns de apresentação de dados (por exemplo, se a extração de dados contiver "123456789", deverá ter como correspondente "\*\*\*\*\*6789", "123456789", "\*\*\*\*\*6789", etc.);
  - 3.14.2. A capacidade de detecção usando palavras e frases-chave totalmente configuráveis;
  - 3.14.3. A capacidade de colocar múltiplas palavras/frases em uma única regra de detecção.
  - 3.14.4. A capacidade nativa de detectar documentos de identificação e números de impostos internacionais, para no mínimo, os países EUA, França e Brasil.
  - 3.14.5. A capacidade de detectar faixas de números válidos para determinados tipos de dados, tal como no mínimo, número de cartão de crédito válido.

#### 4. Terminal do Usuário

- 4.1. Capacidade de descobrir fuga de informações sensíveis, por meio de agente.
- 4.2. Possibilidade de aplicação de políticas mesmo quando o agente não tem comunicação com o servidor de gerenciamento.
- 4.3. Possibilidade de armazenamento em cache, dos arquivos que causaram o incidente até que o usuário se conecte, novamente, à rede corporativa.
- 4.4. A solução possuir a funcionalidade de OCR em arquivos do tipo imagem, no mínimo para:
- 4.4.1. Jpeg;
  - 4.4.2. Bmp;
  - 4.4.3. Png;
  - 4.4.4. Gif;
  - 4.4.5. Tiff.

- 4.5. Monitorar e bloquear dados copiados para dispositivos de armazenamento removível (USB).
- 4.6. A solução deverá possuir capacidade de analisar arquivos menos de 1 kbyte.
- 4.7. Possibilidade de criptografar dados sensíveis copiados para dispositivos USB, sem a necessidade de soluções adicionais.
- 4.8. A solução deve ser capaz de detectar e proteger informações estruturadas de dados, por exemplo, de bancos de dados.
- 4.9. a solução de ponto final deve ser capaz de descobrir e proteger informações estruturadas de dados sem exigir uma conexão com o servidor remoto.
- 4.10. Permitir a monitoração e bloqueio para dados copiados para CD/DVD.
- 4.11. Permitir a monitoração e bloqueio para dados enviados a qualquer tipo de impressora local e de rede.
- 4.12. Permitir a monitoração e bloqueio para ações de copiar e colar.
- 4.13. Permitir a monitoração e bloqueio de dados sensíveis trafegados via e-mail corporativo.
- 4.14. Permitir a monitoração e bloqueio para transmissões HTTPS pelo menos nos seguintes navegadores:
  - 4.14.1. Internet Explorer;
  - 4.14.2. Microsoft Edge;
  - 4.14.3. Mozilla Firefox;
  - 4.14.4. Google Chrome;
  - 4.14.5. Safari.
- 4.15. Permitir a monitoração e bloqueio para transmissões HTTP.
- 4.16. Permitir a monitoração e bloqueio para transmissões via FTP.
- 4.17. Permitir a monitoração e bloqueio para uso de dados confidenciais por qualquer aplicativo, incluindo programas de criptografia não autorizados.
- 4.18. Permitir a monitoração e bloqueio para dados copiados para compartilhamentos de rede pelo Windows Explorer.
- 4.19. A Solução deve possuir monitoramento, por padrão, para pelo menos os seguintes aplicativos:
  - 4.19.1. Chrome;
  - 4.19.2. Firefox;
  - 4.19.3. Internet Explorer (IE);
  - 4.19.4. Microsoft Edge;
  - 4.19.5. Opera;
  - 4.19.6. Safari;
  - 4.19.7. Tor;
  - 4.19.8. Torch;
  - 4.19.9. Acoustica MP3 CD Burner;
  - 4.19.10. Alcohol 120%;
  - 4.19.11. CD-Mate;
  - 4.19.12. Disk Utility;

- 4.19.13. iTunes;
- 4.19.14. Nero Burning ROM;
- 4.19.15. Roxio – Easy Media Creator;
- 4.19.16. Windows Media Player;
- 4.19.17. Amazon Cloud Drive;
- 4.19.18. Box;
- 4.19.19. Dropbox;
- 4.19.20. Egnyte;
- 4.19.21. Google Drive;
- 4.19.22. iCloud;
- 4.19.23. OneDrive;
- 4.19.24. Salesforce Files;
- 4.19.25. ShareFile;
- 4.19.26. Syncplicity;
- 4.19.27. WatchDox;
- 4.19.28. Apple Mail;
- 4.19.29. Eudora;
- 4.19.30. Lotus Notes;
- 4.19.31. MailMate;
- 4.19.32. Microsoft Outlook;
- 4.19.33. Microsoft Outlook Express;
- 4.19.34. Mozilla Thunderbird;
- 4.19.35. Pegasus Mail;
- 4.19.36. Postbox;
- 4.19.37. Sparrow;
- 4.19.38. Windows Live Mail;
- 4.19.39. Windows Mail;
- 4.19.40. DK2 Network Server Remote Monitor - DK2 DESkey;
- 4.19.41. File Encryption XP;
- 4.19.42. Windows Privacy Tray (WinPT);
- 4.19.43. Core FTP LE;
- 4.19.44. Cute FTP Home 8.2;
- 4.19.45. File Transfer Program (Microsoft Utility);
- 4.19.46. FileZilla FTP Client;
- 4.19.47. Flash FXP 3.6 build 1240;
- 4.19.48. FTP Voyager 15;
- 4.19.49. Ipswitch WS FTP Home;
- 4.19.50. Leech FTP;
- 4.19.51. Serv-U;

- 4.19.52. Smart FTP Client;
- 4.19.53. Adium;
- 4.19.54. AIM;
- 4.19.55. Apple Messages;
- 4.19.56. Camfrog;
- 4.19.57. Cisco WebEx;
- 4.19.58. GoToMeeting;
- 4.19.59. ICQ;
- 4.19.60. Jabber Messenger;
- 4.19.61. ManyCam;
- 4.19.62. Microsoft Lync 2010;
- 4.19.63. Miranda IM;
- 4.19.64. ooVoo;
- 4.19.65. Pidgin;
- 4.19.66. Skype for Business;
- 4.19.67. TeamViewer;
- 4.19.68. Teccent QQ;
- 4.19.69. Trillian;
- 4.19.70. Viber;
- 4.19.71. Yahoo! Instant Messenger;
- 4.19.72. Adobe Reader;
- 4.19.73. Bean;
- 4.19.74. Eclipse;
- 4.19.75. Emacs;
- 4.19.76. Evernote;
- 4.19.77. Keynote;
- 4.19.78. LibreOffice/Apache OpenOffice;
- 4.19.79. Mellel;
- 4.19.80. Microsoft Office Access;
- 4.19.81. Microsoft Office Excel;
- 4.19.82. Microsoft Office InfoPath;
- 4.19.83. Microsoft OneNote;
- 4.19.84. Microsoft Office PowerPoint;
- 4.19.85. Microsoft Office Project;
- 4.19.86. Microsoft Office Publisher;
- 4.19.87. Microsoft Office Visio;
- 4.19.88. Microsoft Office Word;
- 4.19.89. Notepad;
- 4.19.90. Numbers;

- 4.19.91. OpenOffice.org Calc;
- 4.19.92. OpenOffice.org Draw;
- 4.19.93. OpenOffice.org Math;
- 4.19.94. OpenOffice.org Writer;
- 4.19.95. Pages;
- 4.19.96. Reminders;
- 4.19.97. Stickies;
- 4.19.98.TextEdit;
- 4.19.99. WordPad;
- 4.19.100. AllegianceMD;
- 4.19.101. eClinicalWorks;
- 4.19.102. ECLIPSY;
- 4.19.103. INGENIX;
- 4.19.104. inteGreat;
- 4.19.105. Sequel;
- 4.19.106. Ares;
- 4.19.107. Azureus;
- 4.19.108. BearShare;
- 4.19.109. BitComet;
- 4.19.110. BitLord;
- 4.19.111. BitTornado;
- 4.19.112. BitTorrent;
- 4.19.113. eMule;
- 4.19.114. FrostWire;
- 4.19.115. Kazaa Lite;
- 4.19.116. LimeWire;
- 4.19.117. Pando;
- 4.19.118. Transmission;
- 4.19.119. uTorrent;
- 4.19.120. 7-Zip File Manager;
- 4.19.121. iArchiver;
- 4.19.122. WinRAR;
- 4.19.123. WinZip;
- 4.19.124. Bluetooth Stack COM Server - BTStackServer;
- 4.19.125. Fsquirt;
- 4.19.126. iTunes;
- 4.19.127. Wireless Link File Transfer App – Irftp;
- 4.19.128. WCESMgr;
- 4.19.129. Aplicor (online);

- 4.19.130. CRM.com;
- 4.19.131. HostAnalytics;
- 4.19.132. Intacct;
- 4.19.133. NetSuite;
- 4.19.134. Oracle CRM on demand;
- 4.19.135. RightNow;
- 4.19.136. Salesforce;
- 4.19.137. WorkDay;
- 4.19.138. FoxPro;
- 4.19.139. Ld;
- 4.19.140. MSTSC;
- 4.19.141. NT backup tool;
- 4.19.142. Vista backup tool;
- 4.19.143. VMWare.

4.20. A solução deve permitir a criação de qualquer aplicativo existente que não venha cadastrado por padrão.

4.21. Definir dispositivos removíveis individuais, ou grupos de dispositivos, como confiáveis e criar exceções de políticas para esses dispositivos.

4.22. A solução deve suportar a integração com o Microsoft RMS (Azure Information Protection), para descriptografar e analisar arquivos do tipo Office (Word, Excel, Power Point entre outros) que foram previamente criptografados pelo Azure RMS ou RD (Active Directory) RMS.

4.23. O agente deverá suportar, no mínimo, Windows 7 (32 e 64 bits), Windows 2008 R2 Enterprise (64bit), Windows 10, Windows Server 2012, Windows Server 2016 e Apple MacOS.

4.24. Todas as funções devem ser executadas por um único agente.

4.25. Permitir a desativação do agente pela console de gerenciamento.

4.26. Possuir mecanismo que reinicie o agente caso o usuário tente interromper o serviço.

4.27. Possuir proteção contra desinstalação do agente.

4.28. Capacidade de apresentar as mensagens de notificações em português.

4.29. Possuir a capacidade de envio de notificação automática, por e-mail, para o usuário e administrador durante a ocorrência de um incidente.

4.30. Possuir a capacidade de gerenciamento da saúde dos agentes.

4.31. Deve permitir a distribuição do agente através de GPO ou por ferramenta de terceiros.

4.32. Deve ter a capacidade de permitir ao usuário justificar a movimentação de conteúdo confidencial, a partir do alerta em “pop-up”, escolhendo opções de justificativa configuráveis pelo administrador da ferramenta.

4.33. O agente deve executar varredura local para verificar se a estação do usuário possui conteúdo confidencial.

4.34. A solução deve ser capaz de proteger informações de impressão digital de dados estruturados offline e sem a necessidade de qualquer comunicação com servidores de administração ou gerenciamento ou repositórios de impressões digitais

4.35. O endpoint deve poder permitir automaticamente a transferência de informações específicas em forma criptografada, configurados pelo administrador;

4.36. O endpoint deve permitir que o usuário defina sua própria senha para criptografia e arquivos criptografados.

4.37. A solução deve permitir que o arquivo criptografado possa ser visualizado ou aberto em computadores onde o endpoint não está instalado usando a senha original do emissor do documento.

4.37.1. Essa funcionalidade deve ser atendida através do próprio agente sem a necessidade de adicionar uma solução de terceiros;

4.38. Deve permitir realizar verificações incrementais, apenas em arquivos novos e alterados.

4.39. Permitir a instalação do agente de modo oculto ou em modo de interação com o usuário.

4.40. Quando utilizado em modo interativo, permitir sincronização de políticas de forma manual, através de acionamento de botão no agente.

4.41. A solução deve suportar integração dinâmica com o User Behavior Analytics ou plataformas UAM.

4.42. Deve permitir incluir na solução de UAM ou User Behavior Analytics a coleta de eventos produzidos pela solução DLP e posterior análise e modelagem realizada pelo UAM ou User Behavior Analytics, com o objetivo de calcular um nível de risco por usuário.

4.43. Deve permitir através do nível de risco obtido pelos algoritmos do UAM ou User Behavior Analytics , esses resultados devem ser devolvidos à solução DLP original para aplicar ações imediatas ou dinâmicas, sem a intervenção humana do administrador da solução.

4.44. Alimentar a console de gerenciamento, com pelo menos, as seguintes informações do agente:

4.44.1. Nome do computador;

4.44.2. IP Address;

4.44.3. Usuário logado;

4.44.4. Última vez que o agente se comunicou com o servidor central;

4.44.5. Identificador do grupo de políticas utilizados;

4.44.6. Campo que informa se o agente está em sincronismo com as últimas políticas/configurações disponibilizadas pelo administrador;

4.44.7. Versão do agente;

4.44.8. Versão da política instalada.

## 5. Incidentes e Respostas

5.1. Deve possuir notificações personalizáveis através de e-mail em caso de violação de política.

5.2. A solução deve permitir ao administrador acrescentar quais detalhes sobre o incidente serão enviados nas notificações.

5.3. Deve permitir tomar ações automáticas pré-definidas na detecção de incidentes, para no mínimo:

5.3.1. Permitir o envio, deletar anexos, quarentena ou criptografar e-mails;

5.3.2. Permitir ou bloquear tráfego de dados sensíveis via FTP;

5.3.3. Permitir ou bloquear tráfego de dados sensíveis via HTTP/HTTPs;

5.3.4. Através do agente, permitir, bloquear ou solicitar justificativa para o tráfego em pelo menos: Qualquer tipo de aplicação executada pelo Sistema operacional, cópia para armazenamentos de rede, impressão de arquivos, E-mails enviados, upload para páginas Web e cópias para dispositivos USB.

- 5.3.5. Permitir a possibilidade de busca ou não de detalhes sobre o incidente durante o registro;
- 5.3.6. Execução de atividades customizadas;
- 5.3.7. Enviar mensagens para servidores de syslog;
- 5.3.8. Enviar notificações por e-mail;
- 5.3.9. Manipular arquivos durante a descoberta de rede.
- 5.3.10. Deve permitir vários botões de resposta na interface gráfica dos incidentes totalmente configuráveis.
- 5.3.11. Os botões de resposta na interface gráfica dos incidentes devem possibilitar no mínimo:
  - 5.3.12. Designar o incidente para resposta de alguém específico;
  - 5.3.13. Modificar o status do incidente;
  - 5.3.14. Modificar a severidade do incidente;
  - 5.3.15. Ignorar o incidente;
  - 5.3.16. Adicionar TAG no incidente;
  - 5.3.17. Adicionar comentários no incidente;
  - 5.3.18. Fazer Download do incidente;
  - 5.3.19. Deletar o incidente;
  - 5.3.20. Acionar scripts ou tarefas customizadas;
  - 5.3.21. Escalar o incidente para o gerente do usuário envolvido;
  - 5.3.22. Escalar o incidente para uma pessoa específica.
- 5.4. Deve exibir todos os detalhes do incidente em uma única página.
- 5.5. Deve permitir exibir partes específicas da mensagem ou arquivo que violou as políticas, através de uma visualização rápida na tela do incidente, sem a necessidade de usar software externo.
- 5.6. Deve permitir armazenar a mensagem e o arquivo original que gerou o incidente.
- 5.7. Deve exibir todo o histórico do incidente, incluindo alterações, edições e respostas executadas automaticamente e manualmente.

## 6. Armazenamento

- 6.1. Deve verificar existência de conteúdo confidencial em file systems sem a necessidade de agentes de coleta (agent-less) para no mínimo CIFS, NFS, SMB e NTFS.
- 6.2. Deve permitir a análise dos file systems através de agentes ou sem agente em sistemas operacionais, para no mínimo:
  - 6.2.1. Windows Server 2008 R2;
  - 6.2.2. Windows Server 2012;
  - 6.2.3. Windows Server 2016;
  - 6.2.4. Red Hat Enterprise Linux 6 e demais releases da versão;
  - 6.2.5. Red Hat Enterprise Linux 7 e demais releases da versão.
- 6.3. Deve analisar conteúdo sigiloso armazenado em ambientes complexos, para no mínimo:
  - 6.3.1. Microsoft Sharepoint;
  - 6.3.2. Lotus Notes;

- 6.3.3. Microsoft SQL Server;
  - 6.3.4. Oracle;
  - 6.3.5. MySQL;
  - 6.3.6. Microsoft Exchange.
- 6.4. Deve analisar conteúdo sigiloso em aplicações em nuvem:
- 6.4.1. Salesforce;
  - 6.4.2. AW;
  - 6.4.3. ServiceNow;
  - 6.4.4. Facebook Workplace;
  - 6.4.5. G-Suite;
  - 6.4.6. Google Cloud Platform;
  - 6.4.7. Azure;
  - 6.4.8. One Drive;
  - 6.4.9. Trello;
  - 6.4.10. Dropbox;
  - 6.4.11. Slack;
  - 6.4.12. GitHub;
  - 6.4.13. LinkedIn.
- 6.5. Deve possuir a capacidade de verificar arquivos Microsoft "PST", possibilitando executar varreduras tanto nas mensagens, assim como, nos arquivos anexos as mensagens.
- 6.6. Possibilidade de mover para quarentena arquivos que violam políticas de segurança.
- 6.7. Deve manter o arquivo no local original, substituindo seu conteúdo por uma mensagem customizável, como aviso e orientação para o usuário.
- 6.8. Permitir a remoção do arquivo que está em quarentena e restaurá-lo de volta ao local original.
- 6.9. Deve permitir coleta automática de arquivos que violem políticas para análise legal (evidência).
- 6.10. Permitir a criação de respostas personalizadas para incidentes.
- 6.11. Exibir detalhes, no incidente, dos arquivos que violam as políticas.
- 6.12. Permitir a visualização das permissões do arquivo.
- 6.13. Deve possibilitar notificação através de e-mail e alerta Syslog em caso de violação de política.
- 6.14. Deve permitir agendamento de varreduras automáticas.
- 6.15. Possuir mecanismo de verificação incremental, na qual apenas arquivos novos, ou alterados, sejam verificados.
- 6.16. Deve permitir configurar janelas de tempo para verificações, interrompendo o processo automaticamente ao fim do período configurado.
- 6.17. Preservar os atributos originais do arquivo, inclusive o atributo "Acessado em", enquanto realiza a verificação.
- 6.18. Possuir capacidade de pausar, manualmente, a verificação.
- 6.19. Deve utilizar técnicas de paralelismo e controle de banda.

- 6.20. Permitir o controle da velocidade das verificações para limitar o uso da largura de banda da rede.
- 6.21. Deve ter a capacidade de reutilizar uma única credencial (nome de usuário/senha) em múltiplos alvos a serem verificados.
- 6.22. Permitir a verificação simultânea em várias fontes distintas.
- 6.23. Permitir limitar quais portas de comunicação serão utilizadas entre o sistema-alvo e o servidor que faz a verificação.
- 6.24. Deve permitir aplicar filtros para verificar na varredura de arquivos de um determinado tipo ou em certo diretório.
- 6.25. Deve permitir aplicar filtros para verificar na varredura de arquivos a idade E/ou o tamanho de arquivos.

## 7. Monitoramento de rede

- 7.1. Permitir a monitoração/bloqueio do e-mail corporativo, evitando que e-mails com dados sigilosos sejam enviados para fora da organização, inclusive em smartphones e tablets.
- 7.2. Possibilidade de colocar mensagens de correio eletrônico em quarentena para análise.
- 7.3. Permitir a monitoração/bloqueio de tráfego WEB, evitando que dados sigilosos saiam da organização por este canal, inclusive em smartphones e tablets.
- 7.4. Capacidade de monitorar/bloquear o tráfego informações sensíveis em posts de redes sociais.
- 7.5. Permitir a monitoração de qualquer protocolo baseado em TCP, como o SMTP, inclusive anexos; HTTP, inclusive arquivos de upload; FTP ativo e passivo.
- 7.6. Capacidade de monitorar o vazamento de dados por meio de softwares de Mensagens Instantâneas.
- 7.7. Permitir a classificação dos protocolos, mesmo quando executados em portas que não são padrão.
- 7.8. Capacidade de filtrar o tráfego da rede para inspeção, segundo o protocolo, faixa de IP e remetente/destinatário de e-mail.

## 8. Classificação da informação

- 8.1. A solução deve ter integração nativa com soluções de Data Loss Prevention;
- 8.2. A solução deve ter capacidade de realizar a rotulagem de informações recém criadas ou pré-existentes sem a necessidade de alterar as propriedades do arquivo, somente seus metadados;
- 8.3. A solução deve ter a capacidade de automaticamente classificar arquivos no mínimo para os seguintes tipos de arquivo;
- 8.3.1. Word, Excel, PowerPoint, Outlook, Project e Microsoft Office;
  - 8.3.2. Open Office;
  - 8.3.3. PDF;
  - 8.3.4. ZIP;
  - 8.3.5. MSG, TIF e EML files;
  - 8.3.6. JPEG;
  - 8.3.7. HTML.

8.4. A solução deve ter a capacidade de proporcionar ao usuário a classificar a informação recém-criada de forma que as soluções integradas possam usufruir desta classificação e incluí-las de forma automática dentro de políticas previamente criadas;

8.5. A solução deve permitir que as soluções integradas detectem os metadados do Classificador, a fim de evitar que o arquivo seja copiado e notificar o usuário/administrador.

8.6. A solução deve possuir integração com o sistema operacional Windows, permitindo que as ações de classificação do usuário sejam logadas pelo sistema operacional;

8.7. A solução deve possibilitar a classificação da informação pelo usuário, possibilitando classificar a informação recém-criada em no mínimo:

- 8.7.1. Informação Pública;
- 8.7.2. Informação Restrita;
- 8.7.3. Informação Interna;
- 8.7.4. Informação Confidencial
- 8.7.5. Informação Pessoal.

8.8. A solução deve possibilitar classificar tanto a informação recém-criada, como pré-existentes;

8.9. A solução deve ter integração para classificação da informação pelo usuário para no mínimo:

- 8.9.1. Word, Excel, PowerPoint, Outlook, Project e Microsoft Office;
- 8.9.2. Open Office;
- 8.9.3. PDF;
- 8.9.4. ZIP.

8.10. A solução deve ser capaz de analisar o comportamento malicioso do usuário, priorizando alertas correlacionados com diversas soluções de segurança em produção, contendo desta forma as ameaças, possibilitando a partir de um único relatório indicar um possível ataque;

8.11. A solução deve ter a capacidade de analisar as informações em conformidade com normas e regulamentações, para no mínimo GDPR, PCI, DSS, SOX, HIPAA;

8.12. A solução deve basear o coeficiente comportamental de risco, indicando a priorização das ações e identificando se o comportamento malicioso é interno ou se é externo, correlacionando para isso informações de no mínimo:

- 8.12.1. Incidentes recebidos da solução de DLP local;
- 8.12.2. Incidentes recebidos pela solução de criptografia, na tentativa de acesso aos dados sensíveis;
- 8.12.3. Incidentes de classificação de documentos/informação por parte do usuário final;
- 8.12.4. Incidentes recebidos da rede de inteligência mundial do fabricante da solução;

8.13. A solução deve ser capaz de identificar os usuários expostos aos maiores níveis de risco e possibilitar a partir desta informação refinar as políticas de proteção dos dados;

8.14. A solução deve permitir que as soluções integradas possam gerar um relatório sobre as marcas de metadados do Classificador, permitindo no mínimo:

- 8.14.1. Localização de arquivo por classificação;
- 8.14.2. Alteração na permissão dos arquivos;
- 8.14.3. Adicionar criptografia no arquivo.

8.15. A solução deve ser capaz de inserir marcações visuais em e-mails (ex. Outlook) para o cabeçalho ou rodapé;

8.16. A solução deve classificar e-mails enviados com arquivos anexados de acordo com a classificação do anexo. Esta classificação deve ser realizada antes do envio.

8.17. solução deve ter a capacidade de calcular a pontuação de risco de cada usuário a partir do comportamento do passado e do presente;

8.18. A solução deve ter a capacidade de criar relatórios de risco, baseados nos maiores infratores;

8.19. A solução deve ter a capacidade de criar políticas de alerta e bloqueio, conforme segue:

8.19.1. Políticas de Alerta: É enviado um alerta ao usuário, no entanto, é possível ao usuário salvar o arquivo e enviá-lo por e-mail;

8.19.2. Políticas de Bloqueio: É enviado um alerta ao usuário, independentemente do nível de classificação do arquivo, onde não será possível salvar, nem tão pouco enviar o arquivo.

8.20. A solução deverá possibilitar no mínimo formas de:

8.20.1. Descoberta de Informações;

8.20.2. O fluxo da informação;

8.20.3. Proteger contra a exfiltração da informação, quer seja intencional, quer seja inadvertida;

8.20.4. Assegurar conformidade com as políticas de acesso e políticas de segurança;

8.20.5. Possibilitar a manutenção da trilha de auditoria por razões de controle e conformidade;

8.20.6. Possibilitar alertar aos usuários quando da criação de informações, sobre as políticas de gerenciamento da informação;

8.20.7. Possibilitar o rastreio de "onde" os dados não estruturados estão sendo criados e "quem" os estão criando;

8.21. A solução deve permitir forçar a aplicação de políticas antes que os dados saiam da gerência do Órgão, para no mínimo:

8.21.1. Políticas de TAG;

8.21.2. Políticas de introdução de cabeçalhos (append headers);

8.21.3. Políticas de inclusão de metadados (add metadata).

8.22. A solução deve ser capaz de implementar gráficos comparativos de risco comportamental entre no mínimo:

8.22.1. Usuários sob o mesmo Gerente;

8.22.2. Usuários do mesmo departamento;

8.22.3. Comportamento dos endpoints;

8.22.4. Comportamento das informações marcadas com TAG de dados sensíveis;

8.22.5. Frequência com que as políticas de proteção dos documentos são violadas;

8.22.6. Envio de informações sensíveis por e-mail e web.

## 9. Relatórios

9.1. A solução deve se integrar nativamente a solução de comportamento dos usuários e correlacionar as informações;

- 9.2. A solução deve exibir informações dos usuários, com pelo menos 20 incidentes durante o período analisado em conjunto com número de correspondências, tamanho da transação, conteúdo e políticas infringidas;
- 9.3. Deve exibir relatórios personalizáveis sobre os incidentes e utilizar filtros, no mínimo de:
- 9.3.1. Ação aplicada;
  - 9.3.2. Responsável pela análise;
  - 9.3.3. Nome da aplicação;
  - 9.3.4. Departamento;
  - 9.3.5. Canal de detecção;
  - 9.3.6. Nível de classificação da informação;
  - 9.3.7. Destino de tráfego da informação;
  - 9.3.8. Tipo estação (Desktop ou Laptop);
  - 9.3.9. ID do incidente
  - 9.3.10. Hora do incidente
  - 9.3.11. Nome do arquivo trafegado;
  - 9.3.12. Histórico do incidente;
  - 9.3.13. Incidentes marcados como ignorados;
  - 9.3.14. TAGs de incidentes;
  - 9.3.15. Quantidade de informação sensível trafegada;
  - 9.3.16. Propriedades do arquivo;
  - 9.3.17. Política acionada;
  - 9.3.18. Nome da regra acionada;
  - 9.3.19. Severidade do incidente;
  - 9.3.20. Origem do incidente;
  - 9.3.21. Status do incidente;
  - 9.3.22. Tamanho da transação;
  - 9.3.23. Dados relacionados as violações encontradas.
- 9.4. Deve exportar relatórios para os formatos HTML, PDF e CSV.
- 9.5. Deve apresentar um painel para visualização dos relatórios.
- 9.6. Deve ter a capacidade para configurar, salvar relatórios e painéis personalizados por usuário.
- 9.7. Deve possuir painéis (Dashboards) para, no mínimo os seguintes itens:
- 9.7.1. Incidentes criados nos últimos X dias;
  - 9.7.2. Políticas mais acionadas;
  - 9.7.3. Incidentes por severidade;
  - 9.7.4. Incidentes por ação tomada;
  - 9.7.5. Incidentes por canais de detecção;
  - 9.7.6. Incidentes por origem/destino;
  - 9.7.7. Usuários que mais violam políticas.



Documento assinado eletronicamente por **Andre Wilson Pimenta Santana, Coordenador de Inovação e Infraestrutura Tecnológica**, em 01/12/2021, às 15:53, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).

---



A autenticidade deste documento pode ser conferida no site <https://sei.funasa.gov.br/consulta>, informando o código verificador **3402349** e o código CRC **0F2EFCC8**.

---

Referência: Processo nº 25100.005982/2021-61

SEI nº 3402349