ASSEMBLEIA LEGISLATIVA
DO ESTADO DE RONDÔNIA
A amiga do rondoniense

Assembleia Legislativa do Estado de Rondônia - ALE/RO

CADERNO DE ESPECIFICAÇÕES TÉCNICAS Nº 0652390/2026/SEC-ADM/SUP-TI/ALERO

ANEXO I	
PROCESSO: 100.173.000006/2026-97	
DOCUMENTOS RELACIONADOS	**OBJETO** - Contratação de solução de 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, incluindo implantação da solução, treinamento e suporte técnico pelo período de 36 (trinta e seis) meses conforme às exigências da Lei Geral de Proteção de Dados (LGPD) constante neste documento e em seus anexos. **ESTUDO TÉCNICO PRELIMINAR (0652379)** **TERMO DE REFERÊNCIA (0652380)**

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

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

1.1 A solução deve ser fornecida em formato de software ou hardware.

1.2 A solução deve permitir instalação em Windows 10/11, Windows Server 2019 ou superior, e macOS 12 ou superior.

1.3 A solução deve fornecer informações sobre operações com arquivos em repouso, em uso e em trânsito.

1.4 A solução deve permitir criação e aplicação de políticas de segurança baseadas em dicionários, palavras-chave e expressões regulares.

1.5 A solução deve suportar OCR para identificação de dados confidenciais em imagens e PDFs.

1.6 A solução deve permitir políticas de bloqueio, notificação, registro ou substituição de regras de DLP.

1.7 A solução deve possibilitar integração com Microsoft 365 (Exchange, SharePoint, OneDrive).

1.8 A solução deve manter logs detalhados de incidentes de segurança e disponibilizar relatórios exportáveis (PDF, XLS, CSV).

1.9 Auditoria de Segurança

1.9.1 A solução deve registrar e auditar atividades de usuários em arquivos, pastas, aplicativos e sites.

1.9.2 A solução deve permitir auditoria de mensagens instantâneas (Teams, Slack, WhatsApp, etc.).

1.9.3 A solução deve permitir integração com ferramentas de Business Intelligence como PowerBI e Tableau.

1.9.4 A solução deve registrar atividades de impressão, cópia, exclusão, upload/download e movimentação de arquivos.

1.9.5 A solução deve notificar o administrador em tempo real sobre violações de política de segurança.

1.10 Informações do Endpoint

1.10.1 A solução deve coletar informações sobre dispositivos, sistema operacional e versão.

1.10.2 A solução deve manter logs sobre conectividade de rede, status da solução e eventos críticos.

1.10.3 A solução deve possuir autodefesa contra adulteração (tamper protection) para impedir desinstalação ou alteração não autorizada.

1.10.4 A solução deve operar em modo offline, mantendo monitoramento mesmo sem conexão com a rede corporativa.

1.11 Proteção de Dados Confidenciais

1.11.1 A solução deve detectar dados confidenciais utilizando dicionários integrados e palavras-chave personalizadas.

1.11.2 A solução deve oferecer Shadow Copy para análise de arquivos envolvidos em incidentes de segurança.

1.11.3 A solução deve aplicar políticas de segurança dinâmicas com base em contexto e comportamento.

1.11.4 A solução deve permitir integração com Azure Information Protection (AIP) e outras marcas de proteção de informações como google Cloud.

1.11.5 A solução deve oferecer restrições de dispositivos externos (USB, Firewire, Bluetooth, etc.).

1.12 Integração com Microsoft 365

1.12.1 A solução deve monitorar operações em OneDrive e SharePoint Online.

1.12.2 A solução deve monitorar e-mails enviados pelo Exchange Online, incluindo Outlook Web e dispositivos móveis.

1.12.3 A solução deve detectar violações de políticas de dados no Microsoft 365 e permitir bloqueio automático de compartilhamentos indevidos.

1.12.4 A solução deve permitir integração com rótulos de classificação e criptografia do Azure Information Protection (AIP)

1.13 UEBA (User and Entity Behavior Analytics)

1.13.1 A solução deve realizar análise comportamental contínua de usuários e entidades.

1.13.2 A solução deve criar perfis de comportamento baseados em histórico (aplicativos, dispositivos, volume de dados, horários de acesso).

1.13.3 A solução deve detectar anomalias em tempo real, como acessos fora do horário, aumento incomum de volume de dados e logins suspeitos.

1.13.4 A solução deve utilizar métodos estatísticos e machine learning para identificar desvios de comportamento.

1.13.5 A solução deve atribuir pontuação de risco (risk score) por usuário/entidade.

1.13.6 A solução deve correlacionar eventos de comportamento com incidentes de segurança (DLP, auditoria, rede).

1.13.7 A solução deve permitir respostas dinâmicas: bloqueio, quarentena ou alerta.

1.13.8 A solução deve gerar relatórios gráficos sobre comportamento e tendências de risco.

1.13.9 A solução deve exportar relatórios em XLS, PDF e CSV.

1.13.10 A solução deve integrar alertas de UEBA com SIEM e SOAR.

1.13.11 A solução deve manter histórico de comportamento de usuários por pelo menos 12 meses.

1.13.12 A solução deve permitir classificação automática ou manual de criticidade de incidentes (alto, médio, baixo).

1.13.13 A solução deve oferecer painéis centralizados com filtros por usuário, entidade, dispositivo e data.

1.13.14 A solução deve oferecer mecanismos de redução de falsos positivos (ajuste de sensibilidade e validação contextual).

1.13.15 A solução deve permitir alertas em tempo real por e-mail ou API.

1.13.16 A solução deve suportar ambientes híbridos (on-premises e cloud).

1.13.17 A solução deve permitir segregação de políticas e perfis por grupos de usuários ou áreas.

1.14. Integração com SIEM

1.14.1 A solução deve exportar logs e eventos para SIEMs de mercado (Splunk, QRadar, ArcSight, LogRhythm, Microsoft Sentinel, etc.).

1.14.2 A integração deve utilizar protocolos padrão (Syslog, CEF).

1.14.3 A solução deve permitir configuração granular de eventos exportados.

1.14.4 A solução deve fornecer dashboards de integração para monitorar o envio de eventos.

1.14.5 A solução deve permitir exportação em tempo real e agendada.

1.14.6 A solução deve disponibilizar documentação técnica oficial para integração com SIEMs.

1.15 ITEM 02 - REPASSE DE CONHECIMENTO

1.15.1 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.

1.15.2 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.

1.15.3 O treinamento deverá ser em Porto Velho – RO, para a equipe técnica do CONTRATANTE ou poderá ser na modalidade remota.

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

1.15.5 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.

1.15.6 Deverá ser ofertada para 1 (uma) turma com no máximo 06 alunos e com carga horária mínima de 16 (dezesseis) horas.

1.15.7 Deverá ser fornecido certificado de conclusão emitido pela Contratada.

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

1.15.9 Deverá ser fornecido material didático completo.

1.15.10 O fabricante da solução deverá emitir declaração informando que a empresa que irá ministrar o treinamento é certificado está apta a minsitrar ou que o mesmo será ministrado pelo proprio fabricante.

1.16 ITEM 03 - CONFIGURAÇÃO E INSTALAÇÃO

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

1.16.2 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.

1.16.3 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;

1.16.4 Caberá à Contratada o irrestrito cumprimento das seguintes prerrogativas:

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

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

1.16.4.3 Instalar e configurar todos os produtos do fornecimento da solução;

1.16.4.4 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;

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

1.17 SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO DURANTE OS 36 MESES

1.17.1 Os serviços profissionais deverão ser executados por equipe certificada pelo fabricante da solução e de forma contínua durante todo o período de vigência de suporte técnico previsto, incluindo suporte remoto com cobertura vinte e quatro horas por dia, sete dias por semana, todos os dias do ano (24x7x365), e gerenciamento fim-a-fim dos chamados na fabricante;

1.17.2 Não serão aceitos profissionais com certificações de nível comercial para a execução desses serviços;

1.17.3 Os serviços poderão ser executados de forma remota ou presencial e em qualquer período (24x7) a ser previamente acordado entre as partes, durante toda a vigência do contrato;

1.17.4 Prestação de serviços de suporte técnico especializado para solução de Data Loss Prevention (DLP), abrange atendimento remoto e/ou presencial, correções de falhas, atualizações, apoio à configuração, tuning e consultoria técnica para operação segura e eficiente do sistema de prevenção à perda de dados.

1.17.5 As atividades contempladas por esse serviço profissional serão:

1.17.5.1 Atendimento a incidentes e dúvidas técnicas relacionados ao funcionamento da solução DLP;

1.17.5.2 Suporte à configuração e reconfiguração de políticas de segurança, conforme evolução das necessidades do órgão;

1.17.5.3 Atendimento a incidentes e dúvidas técnicas relacionados ao funcionamento da solução DLP;

1.17.5.4 Suporte à configuração e reconfiguração de políticas de segurança, conforme evolução das necessidades do órgão;

1.17.5.5 Correção de falhas técnicas (bugfixes);

1.17.5.6 Atualizações evolutivas e corretivas da plataforma (patches, versões estáveis);

1.17.5.7 Apoio técnico para integração com outros sistemas (Active Directory, SIEM, MDM, entre outros);

1.17.5.8 Apoio na análise de eventos e relatórios de segurança emitidos pela solução DLP;

1.17.5.9 Revisões técnicas trimestrais ou semestrais com recomendações e boas práticas de uso;

1.17.5.10 Gestão de licenciamento e dimensionamento, conforme crescimento da infraestrutura ou mudança de cenário regulatório.

1.17.6 O suporte deverá garantir a disponibilidade, segurança, conformidade e continuidade operacional da solução DLP implantada, com suporte técnico adequado ao ambiente e às necessidades da instituição, além de acompanhamento contínuo da efetividade das políticas de proteção de dados sensíveis.

1.17.7 A CONTRATANTE, durante toda a vigência contratual, deverá permitir chamados ilimitados para o suporte técnico;

1.17.8 A abertura do chamado não deverá passar por triagem prévia para posterior atendimento por técnico especializado, devendo ser iniciado diretamente pelo especialista técnico certificado responsável pela investigação e diagnóstico;

1.17.9 No prazo máximo de 10 (dez) dias úteis, contados a partir do dia seguinte à assinatura do Contrato, a CONTRATADA deverá apresentar à CONTRATANTE:

1.17.9.1 As informações sobre os canais de atendimento para contato: número de telefone (0800) ou Service Desk ou endereço de website;

1.17.9.2 As informações referentes ao centro de suporte e assistência técnica responsável pelo atendimento aos serviços de assistência, seja este fornecido pela fabricante dos produtos ou pela própria CONTRATADA, bem como endereço, telefone e e-mail de contato.

1.17.10 O suporte será considerado satisfatório se:

1.17.10.1 Os SLA’s forem cumpridos conforme descrito;

1.17.10.2 A base instalada da solução DLP se mantiver atualizada e funcional;

1.17.11 A ALERO aprovar as interações técnicas mediante pesquisa de satisfação pós-atendimento;

1.17.12 As revisões técnicas forem entregues nos prazos estipulados e com recomendações viáveis.

1.17.13 Deverá ser apresentado carta do fabricante informando que a empresa está apta a prestar serviços de instalação e suporte.

1.17.14 Deverá ser observado e atendido o que se pede no item de manutenção do Estudo Técnico Preliminar.

Documento assinado eletronicamente por **Rafael Ribeiro da Frota**, **Superintendente de Tecnologia da Informação**, em 21/01/2026, às 10:15, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.al.ro.leg.br/validar, informando o código verificador **0652390** e o código CRC **43B1AA09**.

Referência: Processo nº 100.173.000006/2026-97 SEI nº 0652390