MODELO DE PROPOSTA DE COTAÇÃO PARA SOLUÇÃO E DESCRIÇÃO DA SOLUÇÃO

(deve atender aos requisitos apresentados, marcar o tipo de licenciamento e informar os valores conforme quantidade especificada em tabela para período de 36(trinta e seis) meses.)

1. DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

Aquisição de licenças para solução de Gestão, Governança, Monitoração, Auditoria, Automação e Prevenção de Perda de Dados e Arquivos a ser aplicada em serviços como *Active Directory* (AD), Correio Eletrônico (*Microsoft Exchange e Online*), Servidores de Arquivos, *Sharepoint* e *Onedrive*, realizando monitoramento em tempo real, permitindo auditoria, registros, classificação de dados, gerenciando permissionamento/privilégios e identificando comportamentos e possíveis anomalias visando atender requisitos de segurança da informação e normas vigentes como a Lei Geral de Proteção de Dados - LGPD.

A contratação inclui licenciamento, instalação, treinamento, garantia e suporte técnico para a solução, conforme condições, quantidades e exigências estabelecidas neste instrumento.

TIPO DE LICENÇA (marcar a opção)

- ☐ Perpétua
- ☐ Subscrição
- ☐ Outros(especificar):_____

Item	Descrição (Período de 36 meses)	Unidade	Quantidade Mínima	Quantidade Máxima	Valor Unitário	Valor Total
1	Monitoramento e Controle de Acesso - Active Directory (AD)	Usuário	4.500	4.500		
2	Monitoramento e Controle de Acesso - File Server (Windows)	Usuário	4.500	4.500		
3	Monitoramento e Controle de Acesso - e-mail (Microsoft Exchange **on-premises**)	Usuário	1.100	2.000		
4	Monitoramento e Controle de Acesso - e-mail (Microsoft Exchange **online**)	Usuário	3.248	3.400		
5	Monitoramento e Controle de Acesso - Microsoft SharePoint	Usuário	300	900		
6	Monitoramento e Controle de Acesso - *Microsoft OneDrive*	Usuário	200	1.000		
7	Classificação e Descoberta de Dados	Usuário	2.000	4.500		
8	Envio de Alertas de Atividades Suspeitas	Usuário	2.000	4.500		
9	Gerenciamento e Monitoramento de Privilégio de Usuários	Usuário	2.000	4.500		
10	Serviços de Treinamento	Serviço CH	-	-		
Valor Total						

Usuário - refere-se às quantidades aproximadas(estimativa) de usuários que serão monitorados pela solução. (Quantidade de licenças).

Obs. Apresentar carga horária necessária para o item 10 – Serviços de Treinamento tabela abaixo.

Treinamento CH- Carga Horária necessária para cada módulo

Item	Descrição (Período de 36 meses)	Carga Horária Necessária
1	Monitoramento e Controle de Acesso - Active Directory (AD)	
2	Monitoramento e Controle de Acesso - File Server (Windows)	
3	Monitoramento e Controle de Acesso - e-mail (Microsoft Exchange **on-premises**)	
4	Monitoramento e Controle de Acesso - e-mail (Microsoft Exchange **online**)	
5	Monitoramento e Controle de Acesso - Microsoft SharePoint	
6	Monitoramento e Controle de Acesso - *Microsoft OneDrive*	
7	Classificação e Descoberta de Dados	
8	Envio de Alertas de Atividades Suspeitas	
9	Gerenciamento e Monitoramento de Privilégio de Usuários	
Carga Horária Total: _____ **Valor Total do Treinamento: R$ _____**		

2. ESPECIFICAÇÕES DOS REQUISITOS

2.1. REQUISITOS DE NEGÓCIO

Abaixo segue a listagem das principais funcionalidades e características esperadas pela ferramenta.

Da solução:

- Permitir um gerenciamento completo sobre os dados e arquivos, quanto a classificação, propriedade, origem, consumo, restrições e volume (tamanho e quantidade);
- Permitir a análise e classificação de riscos dos dados e arquivos;
- Análise e classificação dos dados, destacando dados confidenciais, sensíveis, sigilosos e restritos;
- Análise preventiva na manipulação e comportamento de arquivos e dados, buscando detectar, indicar e alertar quanto a anomalias, duplicações e possíveis ameaças;
- Alerta de acesso/uso indevido de dados e arquivos classificados como confidenciais, sensíveis, sigilosos e restritos;
- Analisar, proteger, monitorar e gerenciar a integridade das informações armazenadas e disponibilizadas no ambiente do DNIT melhorando mecanismos de:
    - Controle de acesso;
    - Monitoramento de acesso de usuários normais e privilegiados;
    - Estrutura e perfis do Active Directory (AD);
    - Estrutura das permissões de compartilhamento de arquivos;
    - Conformidade de uso dos sistemas com as regulamentações e requisitos de auditoria aplicáveis do DNIT.

- Encontrar arquivos com dados sensíveis, on-premises e/ou na nuvem nos seguintes Ambientes: Windows Server, Sharepoint, OneDrive, Office365, etc;
- Aplicar rótulos e medidas de segurança automaticamente por meio de classificação dos arquivos armazenados em repositórios não estruturados, mapeando onde e para quem os dados estão expostos;
- Gerar metadados importantes para investigação forense, resposta a ataques e vazamentos de informações, bem como a análise comportamental dos usuários internos no ambiente computacional reduzindo ataques internos, perda de informações e má gestão dos repositórios dos dados não estruturados:
    - Quem acessou? Quando? A partir de que máquina? Quais pastas e arquivos foram acessados? Esses arquivos possuem informações sensíveis?
    - Identificação de acessos indevidos de usuários internos mal-intencionados;
    - Dados de LGPD acessados ou compartilhados;
    - E-mails acessados, enviados, marcados como lidos ou não lidos;
    - Pastas criadas abertas, apagadas e renomeadas;
    - Acessos negados;
    - Arquivos compartilhados com pessoas externas através do Sharepoint Online,
    - OneDrive e outros.
    - Quem criou ou habilitou uma conta de usuário, quem definiu uma nova senha e adicionou ou removeu o usuário do grupo de segurança? Quando foi feita esta modificação e que acessos o usuário ganhou?
- Permitir uma melhora nas respostas ao tratamento de incidentes de segurança da informação através do fornecimento de funcionalidades que permitam a rastreabilidade dos eventos, bem como a auditoria dos mesmos, diminuindo os riscos de perda de dados e informações.
- Aumentar o nível de atendimento e qualidade das operações de serviços de TI
- Aprimorar a governança de Dados e de TI.

Do suporte:

- A ferramenta deverá suportar ambientes de rede com servidores Windows e Linux;
- A ferramenta deverá suportar a análise a dados e estruturados e não estruturados;
- O fornecedor deverá dar todo o suporte necessário a instalação e configuração da ferramenta no ambiente de rede do DNIT;

Do uso da solução:

- Treinamento aos usuários da ferramenta quanto ao seu uso e funcionalidades;

Da governança e controle da solução:

- A ferramenta deverá apresentar interface gráfica de fácil uso;
- A ferramenta deverá apresentar as informações em forma de relatórios e gráficos para controle de seu uso bem como dos dados e arquivos.

2.2. REQUISITOS DE IMPLANTAÇÃO

Requisitos de Implantação

A instalação será realizada por técnicos da empresa contratada em conjunto com servidores e colaboradores do DNIT visando sempre o melhor alinhamento possível para evitar quaisquer danos às atividades profissionais da autarquia, principalmente em parada de serviços de rede e e-mail.

A contratada entregará toda a documentação, em meio físico ou eletrônico, necessária para a correta utilização da ferramenta.

Deverão ser estabelecidos processos de atendimento de suporte técnico que garantam a continuidade da execução das soluções.

A implantação das soluções deverá ser realizada através de projeto que siga as boas práticas como PMBOK, Métodos Ágeis e outros compatíveis com a estrutura de TIC do DNIT.

Dos Macro Requisitos Tecnológicos

A instalação ocorrerá em ambiente de rede de dados do DNIT, em servidores Windows Server 2012 (e versões superiores), Linux (CentOS 7 ou superior, Debian 8 ou superior, Ubuntu 12.04 ou superior), operando de maneira proativa no monitoramento de arquivos e dados armazenados e registro de atividades de usuários em arquivos e informações.

A instalação em computadores, do lado cliente (desktops e notebooks), caso necessária, ocorrerá em equipamentos com sistema operacional Windows 10.

Possibilitar o monitoramento e análise de bases de informação sobre usuários, equipamentos e sistemas (Active Directory).

Possibilitar o monitoramento e auditoria em servidor de correio eletrônico (Microsoft Exchange on Premises e Online), inclusive com a possibilidade de gerenciamento e auditoria do repositório de e-mails dos usuários.

Possibilitar identificação e classificação de informações para monitoramento e sinalização em arquivos e possibilitar o mapeamento de onde e para quem os dados são/estão expostos.

Possibilitar a pesquisa em arquivos de termos alfanuméricos (palavras, nomes, etc), visando atender o levantamento de informações sigilosas e sensíveis conforme a Lei Geral de Proteção de Dados - LGPD.

Detecção e investigação (monitoramento) de comportamentos suspeitos em arquivos e informações, buscando reduzir ataques internos, perda de informações e má gestão dos repositórios dos dados não estruturados, com a utilização de alertas e a adoção de reações automatizadas.

Possibilitar ações proativas em casos de incidentes de segurança cibernética e ataque de malwares.

A solução deverá:

Analisar, automatizar tarefas repetitivas, comuns ou complexas, associadas ao gerenciamento e operações em objetos no Active Directory (AD), em servidores de arquivos ou no correio eletrônico;

Analisar o ambiente coletando dados e informações sobre objetos, arquivos e caixas de correio eletrônico, sinalizando-os em caso de comportamento anormal;

Gerar relatórios que permitam o gerenciamento de atividades em objetos, arquivos e caixas de correio eletrônico, registrando histórico e dados de usuários ou recursos (sistemas ou computadores, por exemplo) que praticaram o evento;

Permitir identificar a origem, as permissões e modificação de acesso não necessárias aos objetos, arquivos ou caixas de correio;

Permitir o acesso às informações de auditoria em tempo real ou em histórico de, no mínimo, 5 anos;

Permitir automatizar a identificação, a remoção de permissões, a desativação e a remoção de objetos e arquivos com base em informações de auditoria;

Detectar atividades não autorizadas de processamento de informações;

Permitir a configuração de alertas com base nas informações auditadas, com a adoção de medidas automatizadas para o saneamento do problema;

Utilizar de forma eficiente o espaço em disco necessário para armazenamento dos eventos de auditoria;

Permitir a identificação e classificação de conteúdos confidenciais e sensíveis em servidores de arquivos;

Evitar sobrecarga de processamento dos servidores alvo durante a coleta de informações de auditoria;

Permitir o ajuste os diretórios com herança quebrada de permissões;

Permitir que as autorizações sejam baseadas em necessidades de negócio;

Suportar a versão atual e posteriores do Active Directory (versão atual no DNIT: 2012 R2) e Azure AD, do correio eletrônico (versão atual no DNIT: Exchange 2012) e do serviços de arquivos (versões atuais dos sistemas operacionais: Windows Server 2012 ou superior).

Permitir auditar aproximadamente 4.500 usuários do DNIT ativos no AD.

Permitir auditar aproximadamente 13.600 contas de usuários/sistemas, sendo 4.500 contas de usuários/sistemas ativos no AD.

Permitir auditar aproximadamente 4.700 objetos do tipo grupos do AD.

Permitir auditar aproximadamente 6.600 objetos de computadores/equipamentos do AD.

Permitir auditar aproximadamente 45.700 objetos diversos do AD.

Permitir auditar aproximadamente 80 servidores de arquivos e aplicações existentes no ambiente do DNIT, que armazenam aproximadamente 313 TeraBytes de dados.

Permitir auditar aproximadamente 4.500 caixas de correio eletrônico, sendo aproximadamente 1.100 on premises e 3.400 online.

Permitir auditar aproximadamente 4.500 contas no Sharepoint.

Permitir auditar aproximadamente 4.500 contas no OneDrive.

Suportar a utilização de servidores virtualizados para todos os seus componentes.

Do Treinamento e Capacitação

O treinamento será realizado para cada um dos módulos que compõem a solução ofertada, consistindo na oferta de cursos presenciais ou remotos ou híbridos, e com abordagem prática voltada a todos os requisitos funcionais da solução.

O treinamento deverá abordar de forma teórica e prática todas as funcionalidades solicitadas para cada uma das soluções contratadas, com o objetivo de formar multiplicadores e profissionais capacitados na utilização das funcionalidades.