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. Este Anexo especifica as características técnicas da Solução de Segurança, Auditoria e Governança, contemplando instalação, treinamento e garantia da proteção dos dados da Fundação Nacional de Saúde por 12 meses.

1.1. **Características Gerais**

1.1.1. A solução deve ser capaz de auditar e gerar indicadores de base centralizadas de usuários Active Directory, Servidores de arquivo Microsoft Windows, Microsoft OneDrive;

1.1.2. Os produtos de softwares que irão compor a solução poderão ser licenciados no modelo de direito de uso, desde que:

1.1.2.1. A solução ofertada deverá ser operada por console de interface gráfica única e centralizada;

1.1.2.2. A solução deverá contemplar todas as licenças necessárias para o atendimento de todos os requisitos exigidos nesta especificação técnica.

1.1.3. O software deverá ter certificação utilizada pela administração pública como parâmetro para definição de requisitos de sistema de gerenciamento de segurança da informação, como a ISO/IEC 27.001 ou similares para integridade e confiabilidade jurídica, contratual e regulatória, e pela possibilidade de as informações serem utilizadas para investigações e perícia.

1.1.4. A solução deverá apresentar as seguintes características:

1.1.4.1. Painel web com funcionalidades de pesquisa de auditoria e investigação de eventos anômalos e possíveis ameaças detectadas no ambiente;

1.1.4.2. O painel deve exibir indicadores de interesse relacionados ao ambiente da Funasa expondo ao menos:

- Informações gerais sobre contas como quantidade total, contas de usuários padrão, contas de serviço e contas executivas (presidentes diretores e afins);
- Contas de usuários monitorado com senhas fora de conformidade;
- Contas de usuários que não registraram nenhum evento nos recursos monitorados por um período de tempo maior que 60 dias;
- Grupos de segurança existentes no Active Directory incluindo grupos vazios e em loop; Quantidade e tamanho dos arquivos e pastas existentes nos servidores de arquivos;
- Pastas com inconsistência em suas permissões;
- Pastas expostas no arquivos em nuvem e on premise;
- Pastas expostas pela nuvem;

- Links de compartilhamento criados;
- Pastas e arquivos com dados sensíveis existentes nos recursos monitorados
- Dados parados (sem uso) existente nas bases de dados
- Estações de trabalho com sistemas operacionais desatualizados e defasados.

1.1.5. Permitir autenticação de usuários por meio de senha integrada ao Microsoft Active Directory, AD;

1.1.6. O console de administração deve permitir a configuração de diversos perfis com permissões e restrições de acesso dos usuários às funcionalidades da solução, de forma a segregar o acesso de analistas, equipe de suporte e usuários finais;

1.1.7. Deverá permitir que os perfis de permissões e restrições de acesso sejam determinados por grupos na estrutura do AD.

1.1.8. A solução deverá ser instalada nos sistemas operacionais Windows Server em sua versão 2016.

1.1.9. A solução deverá ser compatível com banco de dados Microsoft SQL Server 2016 ou superior.

1.1.10. Caso seja necessária instalação de agentes nos ativos monitorados, o processo de instalação não poderá gerar indisponibilidade.

1.1.11. A solução deve permitir o acesso a, no mínimo, 5 anos de dados de auditoria capturados e armazenados.

1.1.12. A solução deve suportar a utilização de servidores virtualizados para todos os seus componentes e deve ser compatível com o ambiente de virtualização VMware vSphere no mínimo nas versões 6.4, e 7.0.

1.1.13. A solução deverá possuir escalabilidade suficiente para atender a quantidade de usuários descrito em contrato, sem perda de desempenho e sem acréscimo de licenciamento.

1.1.14. A solução deverá ser capaz de auditar um volume de, pelo menos 50TB de dados.

1.1.15. A solução deve ser capaz de auditar, controlar, monitorar e gerenciar, no mínimo, 7.000 objetos de controladores de domínio sem comprometer o desempenho da solução.

1.1.16. A solução ofertada deve oferecer, com rotinas automatizadas, relatórios agendados e sob demanda, em diversos formatos de arquivos, exportados no momento da geração, ou enviados por e-mail, ou armazenados em um compartilhamento de arquivos através de agendamentos customizáveis.

1.1.17. A documentação relativa às especificações técnicas da solução deverá ser fornecida preferencialmente em português. Caso não exista em português, poderá ser apresentada em língua inglesa. Não há outra possibilidade de língua aceita.

1.1.18. A solução deve permitir o acesso de, pelo menos, 70 colaboradores a todas as suas funcionalidades administrativas. Para funcionalidades que são disponibilizadas a todos os usuários da CONTRATANTE, a solução deve permitir o acesso de todos os usuários contratados.

1.1.19. A solução deve possuir interface nos idiomas português ou inglês.

1.2. **Características Técnicas da Solução**

1.2.1. A solução deverá possuir as funcionalidades de permissionamento, logs, relatórios e análise comportamental dos usuários nos servidores de diretórios de usuários Microsoft Active Directory, e repositórios de arquivos (Microsoft File Server e Microsoft OneDrive) e deverão estar integradas na mesma plataforma e interface de monitoração;

1.2.2. A solução deverá possuir visibilidade da hierarquia do serviço de Diretórios de Usuários através de interface gráfica;

1.2.3. A solução deverá possuir a visibilidade de todos os domínios, Unidades Organizacionais, computadores, grupos e outros objetos do domínio através de uma única interface gráfica e também em formato de relatório;

1.2.4. A solução deverá ter trilha de auditoria classificável e pesquisável de todas as atividades do Active Directory em uma única interface gráfica e também em formato de relatório;

1.2.5. A solução deverá suportar a auditoria dos seguintes eventos do Directory Service:

- Criação de objetos;
- Deleção de objetos;
- Membros adicionados a grupos de segurança;
- Membros removidos de grupos de segurança;
- Modificação de objetos;
- Autenticação de conta;
- Tentativa de reset de senha;
- Bloqueio de conta;
- Desbloqueio de conta;
- Habilitação de conta;
- Desabilitação de conta;
- Permissão adicionada a objeto do AD;
- Permissão removida de objeto do AD;
- Modificação de configuração de GPO;
- Criação de link de GPO;
- Deleção de link de GPO;
- Modificação de link de GPO;
- Requisições Kerberos;
- Requisição de acesso NTLM;
- A solução deverá permitir o gerenciamento de objetos do AD através de sua console;
- Criar novos usuários;
- Criar novos grupos de segurança;
- Alterar parâmetros de usuários já existentes;
- Alterar membros de grupos de segurança;
- Excluir usuários;
- Excluir computadores;
- Reconfigurar senhas;
- Desbloquear usuários;
- Habilitar e desabilitar usuários.

1.2.6. A solução deverá permitir realizar as ações abaixo, em múltiplos usuários, em lotes, ou seja de uma só vez:

- Deleção;
- Reset de senha;

- Desbloqueio da conta;
- Habilitação e desabilitação de conta.

1.2.7. Deve possuir a possibilidade de escolher o método de coleta de eventos de auditoria do AD, por meio de agentes próprios instalados nos domain controller e por meio de coleta dos logs nativos gerados pelo sistema operacional;

1.2.7.1. Em casos de coleta por meio de log nativos, a solução deve coletar, tratar e exibir os eventos sem a necessidade de armazenar o log original do sistema operacional;

1.2.8. A solução deverá permitir a busca por uma pasta nos servidores monitorados e apresentar todos os usuários e grupos de segurança que têm permissões e quais permissões esses objetos têm na pasta.

1.2.9. A solução deverá fornecer todas as funcionalidades citadas abaixo sem a necessidade de retenção dos logs nativos do Windows. Caso a solução ofertada necessite habilitar o log de auditoria do Windows File Server, o hardware sem ponto único de falha necessário para o armazenamento destes logs por no mínimo 12 (doze) meses deverá ser contemplado na proposta.

1.2.10. A solução deverá suportar servidores nas versões Windows Server 2012 ou superior;

1.2.11. A solução ofertada deverá coletar e demonstrar na interface gráfica os eventos de auditoria de todas as operações de abrir, criar, apagar, modificar, renomear e acesso negado dos usuários aos arquivos e pastas dos servidores de arquivos monitorados;

1.2.12. A solução deverá permitir o gerenciamento e alteração das permissões das pastas dos servidores de arquivos monitorados;

1.2.13. A solução deverá permitir a criação de novos grupos de segurança com permissões nas pastas dos servidores de arquivos monitorados;

1.2.14. A solução deverá fornecer funcionalidade de ajuste aos diretórios com herança de permissões quebradas;

1.2.15. A solução deverá possibilitar a criação de pastas que sejam automaticamente reconhecidas na interface gráfica e que possam ser automaticamente usadas pelos usuários;

1.2.16. A solução deverá fornecer a visão das permissões efetivas, ou seja, agregando permissões de Share e NTFS;

1.2.17. A solução deverá coletar, pelo menos, os seguintes eventos de auditoria dos usuários sobre os dados armazenados no OneDrive:

1.2.17.1. pasta criada;

1.2.17.2. pasta apagada;

1.2.17.3. pasta movida;

1.2.17.4. pasta renomeada;

1.2.17.5. pasta copiada;

1.2.17.6. pasta restaurada;

1.2.17.7. convite para pasta criado;

1.2.17.8. convite para pasta apagado;

1.2.17.9. convite para pasta atualizado;

1.2.17.10. convite para pasta aceito;

1.2.17.11. solicitação de acesso para pasta aprovado;

1.2.17.12. link de compartilhamento para pasta criado;

1.2.17.13. link de compartilhamento para pasta atualizado;

1.2.17.14. link de compartilhamento para pasta apagado;

1.2.17.15. link de compartilhamento para pasta usado;

1.2.17.16. arquivo aberto;

1.2.17.17. arquivo modificado;

1.2.17.18. arquivo atualizado;

1.2.17.19. download de arquivo;

1.2.17.20. requisição de acesso ao arquivo aprovada;

1.2.17.21. convite para arquivo criado;

1.2.17.22. convite para arquivo atualizado;

1.2.17.23. convite para arquivo cancelado;

1.2.17.24. convite para arquivo aceito;

1.2.17.25. link de compartilhamento de arquivo criado;

1.2.17.26. link de compartilhamento de arquivo atualizado;

1.2.17.27. link de compartilhamento de arquivo utilizado;

1.2.17.28. link de compartilhamento de arquivo removido;

1.2.17.29. arquivo copiado;

1.2.17.30. arquivo movido;

1.2.17.31. arquivo renomeado;

1.2.17.32. arquivo restabelecido;

1.2.17.33. arquivo apagado;

1.2.17.34. permissões adicionadas;

1.2.17.35. permissões removidas.

1.2.18. A solução deverá possuir relatório de links de compartilhamento no OneDrive;

1.2.19. A solução deverá possuir relatório de dados compartilhados no OneDrive com usuários externos;

1.2.20. A solução deverá possuir relatório de links de compartilhamento para acesso anônimo no OneDrive;

1.2.21. A solução deverá utilizar os eventos coletados pela auditoria para realizar a análise comportamental automática dos usuários de maneira a fazer recomendações de revogação de acesso aos dados não estruturados dos servidores monitorados.

1.2.22. A solução deverá permitir que sejam configurados alertas em tempo real para quaisquer eventos da auditoria habilitada.

1.2.23. A solução deverá permitir que os alertas sejam enviados por e-mail, syslog e SNMP.

1.2.24. A solução deverá permitir a configuração e execução de ações de forma nativa ou através de scripts a partir de qualquer alerta gerado.

1.2.25. A solução deve possibilitar pelo menos o uso de scripts powershell e arquivos .bat como parâmetros para automatização de ações

1.2.26. A solução deverá possuir regras de alertas pré-configurados pelo fornecedor atualizadas frequentemente de eventos suspeitos tais como:

1.2.27.

1.2.27.1. Atividades suspeitas em arquivos e pastas;

1.2.27.2. Grupos de segurança, GPO's e outros objetos do serviço de diretório modificados ou removidos;

1.2.27.3. Detecção de ferramentas de intrusão ou malwares;

1.2.27.4. Acesso suspeitos a dados sensíveis;

1.2.27.5. Escalações de privilégios;

1.2.27.6. Modificação de permissões;

1.2.27.7. Compartilhamento anormal de ativos digitais;

1.2.27.8. Ações em certificados de segurança por usuários não administrativos;

1.2.27.9. Inclusão e exclusão de grupos e usuários no serviço de diretório;

1.2.27.10. Acessos negados;

1.2.27.11. Ataques de sequestro de dados (ransomware);

1.2.27.12. Acessos de localizações geográficas desconhecidas;

1.2.27.13. Acessos de localizações geográficas diferentes em um curto período de tempo (Geo Hopping).

1.2.28. A solução deverá aprender o comportamento padrão dos recursos monitorados e alertar em tempo real quando houver anomalias nestes comportamentos.

1.2.29. A solução deverá ser capaz de identificar desvios de comportamentos quantitativos e desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados por um recurso, assim como identificar eventos suspeitos que tenham ocorrido nas plataformas monitoradas.

1.2.30. Através da análise comportamental, solução deverá realizar a descoberta automática de contas privilegiadas como usuários administrativos , executivos e contas de serviço.

1.2.31. A solução deverá apresentar informações como:

1.2.31.1. Quantidade de alertas e suas severidades em determinado período;

1.2.31.2. Usuários que geraram comportamentos suspeitos;

1.2.31.3. Tipos de alertas mais detectados;

1.2.31.4. Máquinas mais utilizadas para as ações suspeitas;

1.2.31.5. Servidores e pastas que mais sofrem ações suspeitas.

1.2.32. A solução deverá apresentar página com todos os alertas de comportamentos suspeitos gerados pelos usuários, permitindo que seja identificado o cenário do possível ataque.

1.2.33. No painel, a partir de um alerta selecionado, a solução deverá exibir página que liste todos os eventos ocorridos que motivaram a ferramenta a gerar o alerta. A lista desses eventos deve ser personalizável podendo ser filtrada, exibidas ou ocultadas colunas e agregada por valores das colunas exibidas.

1.2.34. A solução deverá fazer análise prévia dos alertas e correlacionar com outras informações e eventos do usuário alertado, dispositivo usado no momento do alerta, horário do evento.

1.2.35. A solução deverá varrer os servidores de arquivos por dados que contém informações sensíveis através da busca em seu conteúdo por informações definidas em dicionários fornecidos pelo fabricante e customizadas pelo usuário.

1.2.36. A solução deverá exibir na mesma interface gráfica todas as permissões dos arquivos e a quantidade de informações sensíveis e qual tipo de informação sensível identificada para facilitar a identificação de potenciais repositórios e pastas expostos.

1.2.37. A solução deverá permitir que a demonstração de todas as pastas dos servidores de arquivos em sua interface gráfica seja filtrada por dados sensíveis;

1.2.38. As informações produzidas pela solução sobre dados sensíveis deverão ser disponibilizadas em forma de relatórios.

1.2.39. A solução deverá permitir que as consultas aos logs de acessos dos usuários às pastas e arquivos sejam filtradas também por dados sensíveis.

1.2.40. A solução deverá permitir a visualização das expressões regulares ou strings que fizeram com que o arquivo fosse considerado sensível diretamente na interface gráfica.

1.2.41. A solução deverá gerar recomendações de revogação de acesso aos dados sensíveis identificados para redução de acesso às informações sensíveis.

1.2.42. A solução deverá integrar a funcionalidade de classificação de dados sensíveis com soluções de terceiros para estender a habilidade de ambos.

1.2.43. A solução deverá permitir integração com ferramentas do DLP (Data Loss Prevention) de classificação de dados sensíveis e informar em relatório onde estes dados se encontram dentro do sistema de arquivos da solução.

1.2.44. A solução deverá permitir a definição das pastas do servidor de arquivos em que os dados sensíveis serão buscados.

1.2.45. A solução deverá permitir definir partes específicas do arquivo a serem analisadas como: partes específicas de arquivos excel (xls), cabeçalho, rodapé e marca d'água de arquivos Microsoft Office, links de arquivos Microsoft Office e PDF.A solução deverá ser capaz de identificar dados que possuam informações referente a Lei de Geral de Proteção de Dados (LGPD): Nome, CPF, passaporte, religião, gênero, nacionalidade;

1.2.46. A solução deverá permitir a definição de agendamento da classificação com hora de início e fim, frequência em que a busca ocorrerá e a data em que deve parar, para que não haja impacto no ambiente.

1.3. **Serviço de instalação para solução de segurança, auditoria e prevenção de ameaças.**

1.3.1. A instalação deverá ser realizada, preferencialmente, em ambiente virtual a ser fornecido pela CONTRATANTE.

1.3.2. A instalação deverá ser precedida de reunião de planejamento com a equipe da CONTRATADA e terá como resultado o plano de instalação, que deverá conter, no mínimo:

- Detalhamento do Escopo;
- Descrição de atividades em cada etapa do projeto;
- Cronograma de atividades;
- Definição de responsabilidades;
- Pontos de controle;
- Descrição detalhada dos componentes;
- Requisitos necessários.

1.3.3. O cronograma deverá contar o prazo em dias corridos para a execução dos serviços e atividades projetadas.

1.3.4. O plano poderá ter propostas de alteração do CONTRATANTE, devendo ser executado somente após a aprovação deste.

1.3.5. A instalação deverá estar em acordo com o especificado para a solução e não poderá acarretar acréscimos de custos de licenciamento para a CONTRATANTE.

1.3.6. Cabe a CONTRATADA entregar a equipe da CONTRATANTE o dimensionamento dos recursos computacionais para os servidores que irão suportar a solução.

1.4. **Treinamento para solução de segurança, auditoria e prevenção de ameaças.**

1.4.1. O treinamento contemplará todos os *softwares* que compõem a solução.

1.4.2. O treinamento deverá ser realizado remotamente.

1.4.3. Caberá à CONTRATADA oferecer os recursos ferramentais para a viabilização do treinamento.

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

1.4.5. O treinamento deverá ser realizado utilizando-se solução idêntica à adquirida pela CONTRATANTE, inclusive quanto à versão dos sistemas;

1.4.6. A carga horária mínima exigida para este treinamento é de 20 horas.

1.4.7. A atividade de treinamento e capacitação deverá ser realizada em dias úteis, com duração máxima de até 6 (seis) horas de instrução diária.

1.4.8. Deverá ser ministrada uma turma de treinamento que terá até 5 participantes.

1.4.9. Deverá ser fornecido material em formato digital ou impresso do conteúdo do treinamento. No caso de material impresso, os custos para impressão e lógica para envio para cada participante são de responsabilidade da CONTRATADA.

1.4.10. Concluídas as atividades de treinamento, a CONTRATADA fornecerá a cada participante que obteve, no mínimo, 80% de presença, um certificado de conclusão que contenha, expressamente, o nome da instituição organizadora, a carga horária do treinamento, o período de realização e o nome completo do participante.

1.4.11. O(s) instrutor(es) deverá(ão) ser comprovadamente certificado(s) nos sistemas e/ou ferramentas fornecidos no escopo da solução.

1.4.12. As datas para a realização das atividades de treinamento e capacitação serão definidas previamente pela CONTRATANTE, respeitados os prazos de vigência da garantia.

1.4.13. O público-alvo deste treinamento são os analistas responsáveis pela execução de atividades de administração e auditoria dos ambientes monitorados pela solução. Os participantes serão indicados pela CONTRATANTE.

1.4.14. A qualidade do treinamento deverá ser avaliada por seus participantes ao seu final e, caso seja considerada insuficiente, a CONTRATADA deverá providenciar a realização de nova turma, até o alcance dos objetivos do treinamento, sem ônus adicional para a CONTRATANTE.

1.4.15. Caso alguns dos prazos previstos e acordados para a execução do treinamento não sejam cumpridos por responsabilidade da CONTRATADA, ela estará sujeita às sanções previstas neste termo de referência.

Documento assinado eletronicamente por **Andre Wilson Pimenta Santana**, **Integrante Requisitante**, em 01/11/2022, às 11:04, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Gleicy Kellen dos Santos Faustino**, **Integrante Técnico**, em 01/11/2022, às 12:03, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Haroldo Rodrigues da Silva**, **Pregoeiro(a)**, em 01/11/2022, às 14:55, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.