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 Técnicas Gerais

1.1.1. A solução deve ser capaz de auditar e gerar indicadores de base centralizadas de usuários Active Directory e Servidores de arquivo Microsoft Windows assim como estações de trabalho Microsoft Windows;

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 poderá ser composta por mais de um software, desde que o conjunto atenda a todos os requisitos Técnicos e Funcionais;

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. Ainda que a solução seja composta por mais de um produto de software, os consoles de administração deverão compartilhar as seguintes características:

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

1.1.3.2. 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 a grandes grupos de usuários;
- Estações de trabalho com sistemas operacionais desatualizados e defasados;
- Estações de trabalho em situação de vulnerabilidade;

1.1.4. Permitir autenticação de usuários por meio de senha integrada ao Microsoft Active Directory, AD, ou a outros serviços de diretórios que sejam compatíveis com o protocolo *Lightweight Directory Access Protocol* em sua versão 3 ou superior;

1.1.5. 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;

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

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

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

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

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

1.1.11. 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.

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

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

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

1.1.15. 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.

1.1.16. 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.

1.1.17. A solução deve permitir o acesso de, pelo menos, 50 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.

1.1.18. A solução deve possuir interface nos idiomas portugues ou inglês.

1.2. **Características Técnicas para solução de Proteção das Bases Centralizadas;**

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 deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios de dados;.

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 as ações abaixo em múltiplos usuários de uma só vez:

- Deleção;
- Reset de senha;
- Desbloqueio da conta;
- Habilitação e desabilitação de **conta.**

1.2.7. Possuir as funcionalidades de permissionamento, logs, relatórios e análise comportamental dos usuários descritas nos itens acima em plataformas de servidores de arquivos Windows;

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 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.

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

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

1.2.20. A solução deverá permitir a configuração e execução de ações préconfiguradas ou através de scripts a partir de qualquer alerta gerado.

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

- Atividades suspeitas em arquivos e pastas;
- Grupos de segurança, GPO’s e outros objetos do serviço de diretório modificados ou removidos;
- Detecção de ferramentas de intrusão ou malwares;
- Acesso suspeitos a dados sensíveis;
- Escalações de privilégios;
- Modificação de permissões;
- Inclusão e exclusão de grupos e usuários no serviço de
- diretório;
- Acessos negados;
- Ataques de sequestro de dados (*ransomware*).

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

1.2.23. 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.

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

1.2.25. A solução deverá apresentar informações como:

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

1.2.27. Usuários que geraram comportamentos suspeitos;

1.2.28. Tipos de alertas mais detectados;

1.2.29. Máquinas mais utilizadas para as ações suspeitas;

1.2.30. Servidores e pastas que mais sofrem ações suspeitas.

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

1.2.32. 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.

1.2.33. 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.

1.2.34. 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.

1.2.35. 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.

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

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

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

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

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

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

1.2.42. 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.

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

1.2.44. 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.

1.2.45. 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. **Características Técnicas para solução de Proteção Estações de Trabalho**

1.3.1. A solução deve ser compatível com os seguintes sistemas Operacionais:

1.3.1.1. Windows 7 em 32 e 64 bits;

1.3.1.2. Windows 10 em 32 e 64 bits;

1.3.1.3. Windows 11 em 32 e 64 bits;

1.3.2. A solução deve prover detecção automatizada dos incidentes de segurança fornecendo informações detalhadas sobre o incidente ou vulnerabilidade para pronta ação de contenção e resposta, disponibilizando a informação em seus níveis de criticidade tanto no dashboard, em tempo real quanto em seu histórico por meio de relatórios;

1.3.3. A distribuição e instalação dos agentes deve realizar ao menos:

- Descoberta automática dos endpoints que não possuem o agente instalado;
- Descoberta automática e evidenciação dos agentes que eventualmente tenham sido paralisados propositadamente;
- Instalação remota via Group Policy (GPO), Web e console de gerenciamento.

1.3.4. A solução deve ser capaz de detectar quais estações possuem o agente instalado e sua versão. Caso a solução possua uma versão de agente mais atual, deve realizar a atualização de forma automatizada;

1.3.5. Os agentes devem possuir proteção contra desinstalação ou interrupção do agente;

1.3.6. Deve detectar e analisar, automaticamente e em tempo real por aprendizado de máquina (“Machine Learning” ou “Deep Learnig”) e análise comportamental;

1.3.7. Possuir capacidade de aprendizado de comportamento de usuários para aprimoramento das detecções de comportamentos suspeitos.

1.3.8. Deve possuir tecnologia de análise de arquivos binários para identificação de comportamento malicioso.

1.3.9. Capacidade parametrizada de coletar, registrar e armazenar todas as conexões (TCP) ou transmissões (UDP) de rede, incluindo informações sobre endereços IP, portas de origem e destino e domínios DNS;

1.3.10. Informar programas e processos em execução em tempo real;

1.3.11. Possuir registro de softwares (instalados, executados e em execução), com possibilidade de mitigação de softwares vulneráveis em execução bem como a data de instalação de cada item.

1.3.12. Monitorar e alertar sobre arquivos e programas suspeitos e maliciosos na rede, bem como a utilização de recursos elevados do endpoint ou sistema operacional;

1.3.13. Detecção de malwares por comportamento utilizando assinaturas;

1.3.14. Detecção de código malicioso por análise comportamental;

1.3.15. Realizar identificação de propagação de malwares tipo ransomware e atividades suspeitas de criptografia de arquivos;

1.3.16. Possuir motor de análise e detecção de dados acessados pelo usuário, em trânsito, para fora ou dentro da rede e armazenados localmente ou em um compartilhamento de rede;

1.3.17. Emissão de alertas no Console Centralizado indicando uma nova classe de dispositivo encontrada, ao identificar um novo dispositivo conectado na estácào, cujo hardware seja desconhecido (alerta de alteração de hardware);

1.3.18. Monitoramento e coleta de eventos de logon e logoff de usuários, bloqueio e desbloqueio de sessão e acessos a compartilhamentos;

1.3.19. Monitoramento de páginas web acessadas e upload e download de arquivos a partir de páginas web;

1.3.20. Possuir monitoramento de acesso remoto aos endpoints, de acordo com configuração realizada, de forma centralizada, via gerenciador da solução;

1.3.21. Possuir monitoramento de operações (acesso, cópia, modificação, duplicação e exclusão) com arquivos no disco local, dispositivos USB, dispositivos móveis conectados, drives CD/DVD, mídias removíveis, compartilhamento em rede ou em nuvem e acesso a drivers de rede, com a respectiva coleta de evidências;

1.3.22. Realizar monitoramento, emissão de alertas e bloqueio automático ou manual de softwares não autorizados;

1.3.23. Identificação de patches não aplicados em sistemas operacionais e softwares instalados em endpoints;

1.3.24. A solução deverá monitorar e informar os recursos de segurança dos *endpoints* em dashboard e relatórios contendo, no mínimo, as seguintes informações:

- Dados sobre existência e atualizações do antivírus;
- Situação do firewall no *endpoint*;
- Se há *antispyware* instalado e se está atualizado;
- Qual é a versão do sistema operacional;
- Métricas de uso de CPU, memória RAM e rede.

1.3.25. Todos os registros de eventos classificados como incidentes deverão ser passiveis de envio ao gerenciador da solução;

1.3.26. Monitoramento e detecção dos seguintes atributos de hardware e software:

- versões;
- número de série;
- fabricante; e
- datas.

1.3.27. Localização imediata do primeiro software instalado na rede.

1.3.28. Monitoramento e detecção da performance dos endpoints, contemplando dos seguintes atributos:

1.3.29. Monitoramento e detecção de processos, drivers e serviços:

1.3.30. Identificação de novo processo e localização da primeira ocorrência;

1.3.31. Identificar processos suspeitos através de análise comportamental;

1.3.32. Identificação de alteração de comportamento de processo, através de mudança de registro de versão, hash, assinatura, nome original, checksum e etc.

1.3.33. Permitir a coleta de, no mínimo, as seguintes informações para investigação, sendo remoto ou não:

- Arquivos escritos;

- Arquivos copiados para dispositivos de armazenamento externo e vice-versa;
- Falhas de logon e logoff;
- Logins paralelos
- Tentativa de resolução de hostname;
- Tentativa de acesso a URL;
- Logs do Windows com eventos de aplicação, segurança e sistema;
- Identificação de acesso remoto via processos, IP e conexões internas ou externas e etc.
- Histórico de usuários que realizaram logon no equipamento;
- Portas de rede ativas;
- Hash MD5, SHA1, SHA2 e SHA3;
- Processos na memória;
- Processos usando a API do Sistema Operacional;
- Contas de usuários;
- Listagem de volumes;
- Tarefas do Sistema Operacional.

1.3.34. Possuir alimentação automática ou manual de fontes externas de inteligência para detecção e combate a novas ameaças e ataques (threat intelligence);

1.3.35. Possuir mecanismo automático de priorização de ameaças, fornecendo insumos para que infecções mais graves sejam investigadas prioritariamente;

1.3.36. Ter funcionalidade de identificar ameaças através de correlação de eventos e comportamentos dos endpoints gerenciados;

1.3.37. Deve gerar relatórios a partir de todos os dados monitorados;

1.3.38. Deve permitir filtros personalizados para facilitar a visualização e gerenciamento;

1.3.39. Deve gerar relatórios automatizados em períodos, por hora, por dia, por semana, por mês e por ano, configuráveis pelo administrador;

1.3.40. Os relatórios devem ser gerados em, pelo menos, formato XML para permitir a correlação e comparação com outras tabelas.

1.3.41. Relatórios devem conter, no mínimo:

- Informações por domínio;
- Informações por grupo de endpoints;
- Informações por usuário (atividade web, uso de aplicativos e produtividade);
- Informações por estação ou grupo de estações;
- Informações de ataques identificados;
- Informações de logon e logoff de usuários nos endpoints, inclusive logons secundários e em cache, além de bloqueios e desbloqueios de sessão;
- Informações de arquivos (modificados, excluídos, copiados, acessados e duplicados);
- Informações de programas (instalados, executados e em execução);
- Informações de arquivos copiados dos discos locais dos endpoints para dispositivos de armazenamento externo e vice-versa;
- Informações de histórico de ocorrências quanto ao uso simultâneo de redes WIFI e cabeadas por máquina ou por usuário;

- Inventário de hardware e dispositivos;
- Atividade de impressora quanto ao uso, ordem de impressão e arquivos enviados para impressão;
- Performance das máquinas;
- Estatística da rede;
- Informações sobre ocorrência e irregularidade de processos;
- Fluxo de arquivos .pdf, .doc, .xlm, configuração e etc.

1.3.42. Fornecer relatório de computadores com serviços da ferramenta não conformes, com versões de componentes inconsistentes, com varreduras desatualizadas e com políticas e configurações incorretas;

1.3.43. Fornecer resumo geral sobre status de segurança dos endpoints (antivírus, Firewall do Windows, falta de atualização de segurança do Windows e computadores desprotegidos);

1.3.44. Deve ter um sistema de notificações e alertas personalizável pelo administrador que poderá configurar os itens constantes no alerta, como:

- infecções detectadas;
- arquivos acessados, copiados, apagados e alterados;
- atividades de mídias removíveis (USB);
- alteração de hardware;
- utilização de redes sem fio e cabeada;
- avisos sobre eventos críticos no sistema (falha de hardware, falta de espaço de armazenamento em disco, notificação de ataque, etc.)
- instalação de novos aplicativos.

1.3.45. Deve ser capaz de registrar ou notificar os alertas e dados nativamente de forma automatizada;

1.3.46. Deve possibilitar alertas por e-mail, para um destino definido pelo administrador;

1.3.47. Possuir capacidade de apresentar os alertas em interface web;

1.3.48. Capaz de emitir alertas baseados na comparação de hashes criptográficos de executáveis com blacklists, fornecidas pela própria solução, caso um executável considerado malicioso seja executado em um ou mais computadores;

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

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

1.4.2. 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.

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

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

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

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

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

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

1.5.2. O treinamento deverá ser realizado remotamente.

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

1.5.4. 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.

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

1.5.6. A carga horária mínima exigida para este treinamento é de 30 horas.

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

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

1.5.9. 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.

1.5.10. 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.

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

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

1.5.13. 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.

1.5.14. 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.

1.5.15. 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 20/10/2022, às 14:25, 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 20/10/2022, às 14:50, 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 20/10/2022, às 15:20, 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 **Alan Oliveira Lima**, **Diretor do Departamento de Administração**, em 20/10/2022, às 16:05, 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 **Miguel da Silva Marques**, **Presidente**, em 20/10/2022, às 18:02, 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 **3966749** e o código CRC **CE479A7E**.

Referência: Processo nº 25100.004170/2022-80 SEI nº 3966749