

The logo for FNDE (Fundo Nacional de Desenvolvimento da Educação) features the acronym 'FNDE' in a bold, blue, sans-serif font. A horizontal yellow bar is positioned directly beneath the letters.

Fundo Nacional  
de Desenvolvimento  
da Educação

**Implantação de Auditoria para o Ambiente  
Microsoft nos Serviços de AD, File Server e  
Exchange Server do FNDE**

**Planejamento da Contratação**

***Especificações Técnicas***

**Versão 3.0**

## ÍNDICE

|   |    |
|---|----|
| I – OBJETO .....  | 3  |
| II – ESPECIFICAÇÃO.....                                     | 3  |
| III – CONDIÇÕES DE ENTREGA E/OU FORNECIMENTO .....          | 10 |
| IV – CONDIÇÕES DE RECEBIMENTO E PAGAMENTO .....             | 11 |
| V – MOTIVAÇÃO .....   | 12 |
| ENCARTE C – Condições de manutenção e suporte técnico ..... | 15 |

## **I – OBJETO**

**I.1.** Prestação de serviços para fornecimento de solução baseada em software para ambiente Microsoft, com vistas à implantação de auditoria, controle e gerência de permissionamento dos serviços de AD (Microsoft Active Directory), servidor de Arquivos (Microsoft File Server) e sistema de correio eletrônico (Microsoft Exchange Server) do órgão, bem como execução de serviços de planejamento e consultoria, implementação e testes, além de transferência de conhecimentos, com garantia (manutenção e suporte técnico), de acordo com as condições e especificações constantes neste Documento e em seus respectivos Encartes.

**I.2.** São produtos esperados pela contratação:

**I.2.1.** Solução baseada em softwares para auditoria, controle e gerência de permissionamento dos serviços de AD (Microsoft Active Directory), servidor de Arquivos (Microsoft File Server) e sistema de correio eletrônico (Microsoft Exchange Server);

**I.2.2.** Serviços de planejamento e consultoria e de implementação e testes;

**I.2.3.** Serviços de transferência de conhecimentos;

**I.2.4.** Garantia (manutenção e suporte técnico).

**I.3.** São resultados esperados com a contratação:

**I.3.1.** Visão completa da estrutura do AD, devendo ser possível administrar seu repositório de usuários e grupos de segurança através de uma interface única, juntamente com a gestão de seus servidores de arquivos;

**I.3.2.** Auditoria eficiente do Active Directory e Exchange, que por meio dos logs de auditoria você tem visibilidade de todos os eventos ocorridos;

**I.3.3.** Gestão do permissionamento e dos logs de todas as plataformas monitoradas em uma única console;

**I.3.4.** Relatórios visando facilitar o controle sobre o que acontece em todos os ambientes;

**I.3.5.** Alertas de modificação, quando alguma ação for disparada;

**I.3.6.** Consultas e pesquisas de eventos;

## **II – ESPECIFICAÇÃO**

### **II.1. Objetivo**

**II.1.1.** O objetivo desta contratação é de se efetuar a implantação de uma solução de auditoria, controle e gerência de permissionamento dos serviços de AD (Microsoft Active Directory), servidor de Arquivos (Microsoft File Server) e sistema de correio eletrônico (Microsoft Exchange Server), os quais são responsáveis pela comunicação e armazenamento dos dados não estruturados do FNDE, contemplando:

**II.1.1.1** Licenciamento para o mínimo de 2.000 (dois mil) usuários internos;

**II.1.1.2** Licenciamento para o mínimo de 2.000 (duas mil) caixas postais;

**II.1.1.3** Instalação e configuração da solução (softwares) para o ambiente Microsoft;

**II.1.1.4** Integração e compartilhamento de recursos e auditoria, controle, gerenciamento e permissionamento da solução com o ambiente de produção existente;

**II.1.1.5** Execução de serviços profissionais para planejamento e consultoria, implementação e testes;

**II.1.1.6** Transferência de conhecimentos; e

**II.1.1.7** Garantia: serviço de manutenção e suporte pelo período de 36 (trinta e seis) meses;

## **II.2. Descrição detalhada da Solução**

### **II.2.1. Características funcionais:**

**II.2.1.1** A solução ofertada deverá reter as informações de log e histórico em banco de dados (MS SQL ou Oracle), por um período que será determinado na fase de escopo do projeto (mínimo de 12 meses);

**II.2.1.2** A solução deve fornecer todas as funcionalidades citadas sem o acionamento dos logs nativos do Windows. Caso a solução ofertada habilite log de auditoria do Windows, o hardware necessário para o armazenamento destes logs por 12 (doze) meses deverá ser contemplado na proposta;

**II.2.1.3** A solução deverá contemplar na mesma console a possibilidade de englobar as funcionalidades através de agentes adicionais para no mínimo as plataformas Linux, Microsoft Active Directory, Microsoft Exchange Server e Windows Server;

**II.2.1.4** Caso a solução utilize um agente nos servidores a serem monitorados, sua instalação não deve requerer a reinicialização dos mesmos;

**II.2.1.5** O agente deve possuir um mecanismo de monitoramento de desempenho (performance) dos servidores onde atua, de modo a não permitir que o nível de consumo de processamento pelo agente nos servidores ultrapasse de 5% de consumo de CPU;

**II.2.1.6** A solução deverá prover informações de quem acessa quais dados, quem está acessando ou tentando acessar os dados, qual tipo de acesso foi feito, quem acessou ou deveria ter acesso aos dados, quem não está utilizando o permissionamento atual, quais dados são menos acessados, e quem deu ou revogou permissões de acesso;

**II.2.1.7** A solução deve fornecer método para assinalar ou associar um usuário como "Proprietário" de uma pasta ou grupo;

**II.2.1.8** Deve permitir a Importação/exportação dos Proprietários das informações de/para uma lista, e permitir o upload de um arquivo contendo informações para a designação do proprietário de cada pasta;

**II.2.1.9** Deve permitir o gerenciamento das funcionalidades através de console própria ou navegador WEB;

**II.2.1.10** Fornecer interface única de usuário para exibir as permissões, os detalhes da auditoria, as estatísticas de acesso a dados e alertas;

**II.2.1.11** A solução deve suportar a utilização de servidores Virtualizados (VMWare) para todos os seus componentes;

**II.2.1.12** A solução deve contemplar o licenciamento dos bancos de dados e sistemas operacionais para a instalação e monitoração da solução;

## **II.2.2. Permissionamento**

**II.2.2.1** A solução deverá integrar com administradores de usuários, grupos de usuários e permissionamento de plataformas AD (Microsoft Active Directory) LDAP, NIS e usuários locais dos servidores, bem como monitorar estas bases;

**II.2.2.2** A solução deverá mostrar em uma mesma interface toda a base de usuários e de dados monitorados, exibindo para cada pasta ou arquivo a visualização gráfica interativa das listas de controle de acesso incluindo grupos, sub-grupos e seus respectivos membros;

**II.2.2.3** Esta mesma interface deverá mostrar os níveis de permissões das pastas que o usuário tem acesso, dar visibilidade de todos os objetos que um usuário ou grupo tenham permissões para acessar, incluindo herança de permissões ativa/desativada e indicação de compartilhamento;

**II.2.2.4** A solução deve permitir a visibilidade bi-direcional de quais pastas podem ser acessadas por quais usuários e na direção contrária, indicando todos as pastas onde o usuário tem acesso e qual tipo de acesso (leitura, escrita, modificação), sem afetar o ambiente em operação;

**II.2.2.5** A ferramenta deverá prover filtros para visualizar todos os objetos de dados de forma gráfica incluindo pastas protegidas e únicas;

**II.2.2.6** A solução deverá fornecer a visão das permissões efetivas, ou seja, agregando permissões de Share e NTFS;

**II.2.2.7** A ferramenta não deve restringir a quantidade das listas de acesso (ACLs) coletadas e/ou armazenadas;

**II.2.2.8** A visualização de grupos deve compreender todos os grupos filhos (sub-grupos) sem restrição de número de hierarquias;

**II.2.2.9** A solução deve possibilitar a configuração de uma credencial diferente para cada volume a ser monitorado;

**II.2.2.10** A solução deverá realizar a modificação das permissões dos usuários no Microsoft Active Directory através de autenticação de usuário e senha dos administradores do AD com efetivação imediata e possibilitar o agendamento para data futura;

**II.2.2.11** A solução deverá trabalhar integrada ao AD sem a necessidade de inserção de usuários manual, e fornecer a habilidade para corrigir permissões e modificar grupos via interface gráfica;

**II.2.2.12** A solução deve permitir a modelagem de dados e alteração do perfil de acesso, para avaliação de impactos, antes da execução em ambiente real, identificando quais usuários acessam determinada pasta e perderão ou ganharão acesso nesta modelagem;

**II.2.2.13** A solução deve permitir a modelagem de permissionamento de maneira gráfica, incluindo a simulação do impacto de mudanças no permissionamento de grupos e usuários, e da remoção de permissões excessivas, inclusão de novos grupos e identificação de quais usuários serão afetados com estas trocas de permissões;

### **II.2.3. Log**

**II.2.3.1** A solução deve coletar o log de forma normatizada dos repositórios de dados em plataforma Windows, Linux, Sharepoint e Microsoft Exchange;

**II.2.3.2** A solução ofertada deve manter o log das operações de abrir, criar, apagar, modificar, copiar, renomear e acesso negado;

**II.2.3.3** O log da solução ofertada deve conter informações completas de cada uma das operações com data e horário, nome do servidor de arquivos, tipo do objeto, caminho (path) dos dados, domínio, destino da movimentação, arquivo impactado e nome do usuário;

**II.2.3.4** Deverá permitir filtragem gráfica, ordenação e agrupamento dos logs;

**II.2.3.5** A solução deverá identificar em uma mesma tela todas as atividades de um determinado usuário ou determinada pasta de todos os repositórios monitorados e diretórios de usuários;

**II.2.3.6** Fornecer resumo gráfico das atividades auditadas, incluindo:

- (a). Visualização dos usuários mais e menos ativos;
- (b). Visualização dos diretórios mais e menos ativos;
- (c). Visualização dos diretórios onde um usuário ou um grupo de usuários estejam acessando;
- (d). Visualização dos usuários que estejam acessando um diretório;
- (e). A ferramenta deve normatizar eventos relacionados e apresentar como um único evento para o mesmo objeto;
- (f). A solução deve permitir auditoria direta de quem tem acesso aos dados na tela da console, sem necessidade de gerar relatório demonstrativo;

### **II.2.4. Relatórios**

**II.2.4.1** A solução ofertada deve gerar relatórios nos formatos TXT, CSV, HTML, XLS e PDF;

**II.2.4.2** A ferramenta deve permitir o agendamento para envio de relatórios pelo correio eletrônico;

**II.2.4.3** Os relatórios agendados devem poder ser entregues tanto via e-mail quanto em uma determinada pasta do servidor sem a necessidade de customização adicional;

**II.2.4.4** O envio dos relatórios por e-mail deve ser feito a partir da própria solução, ou seja, sem a utilização de software de terceiros e deve suportar o protocolo SMTP;

**II.2.4.5** A ferramenta deve possibilitar a definição da prioridade de cada relatório agendado;

**II.2.4.6** A ferramenta deve fornecer relatórios customizáveis sob demanda e agendados;

**II.2.4.7** A ferramenta deve fornecer relatório dos acessos aos arquivos;

**II.2.4.8** A ferramenta deve armazenar todas as modificações feitas nas permissões dentro e fora da interface gráfica;

**II.2.4.9** Fornecer relatórios sobre onde permissões concedidas a grupos globais (Everyone, Domain Users, Users) estão sendo utilizadas;

**II.2.4.10** Armazenar todas as modificações em grupos feitas dentro e fora da interface gráfica;

**II.2.4.11** Fornecer relatórios de grupos de segurança vazios ou não utilizados;

**II.2.4.12** Fornecer relatórios de SIDs não resolvidos e usuários com permissão direta em pastas;

**II.2.4.13** Fornecer relatórios de dados e usuários inativos;

**II.2.4.14** Fornecer relatórios sobre administradores acessando dados de negócio;

**II.2.4.15** Fornecer relatórios de usuários desabilitados que ainda fazem parte de grupos de segurança;

**II.2.4.16** Fornecer relatório que mostre quais eram as permissões para determinada pasta em uma data passada sem a necessidade de um processo manual para guardar as permissões a serem recuperadas;

**II.2.4.17** Possibilitar o direito de revisão de gestão de dados através de relatórios indicativos do uso dos dados;

**II.2.4.18** Suprir com rotinas automatizadas, relatórios programados e outras facilidades os benefícios esperados, destes relatórios;

**II.2.4.19** A solução deve ser capaz de fornecer relatórios para auditoria e conformidade (compliance);

## **II.2.5. Análise Comportamental**

**II.2.5.1** A ferramenta deve realizar a análise comportamental dos usuários de maneira a fazer recomendações de alteração, revogação de acesso, trocas de grupos e permissões aos dados não estruturados e semiestruturados dos servidores monitorados;

**II.2.5.2** A solução deve identificar, de forma automática, usuários com acesso a pastas e/ou arquivos indevidos sugerindo a revogação de acesso;

**II.2.5.3** A solução deverá fornecer em modo gráfico recomendações sobre permissionamento excessivo, baseado na análise de atividade de acesso;

**II.2.5.4** Fornecer identificação gráfica de atividades de acesso anormais;

**II.2.5.5** Estas recomendações deverão também ser fornecidas em forma de relatório;

## **II.2.6. Alertas**

**II.2.6.1** A ferramenta deve realizar análises e gerar alertas de comportamentos suspeitos como leitura ou gravações em excessos que diferem do comportamento normal do usuário;

**II.2.6.2** A notificação deverá ser feita também via e-mail;

**II.2.6.3** A ferramenta deve emitir um alerta quando um usuário desviar do seu comportamento padrão;

**II.2.6.4** A ferramenta deve alertar quando um usuário tentar acessar uma pasta a qual ele não tem acesso;

**II.2.6.5** Fornecer relatórios sobre atividades de acesso anormais;

## **II.2.7. Microsoft AD (Active Directory)**

**II.2.7.1** A solução deve efetuar as funcionalidades de permissionamento, Log, Relatórios, Análise Comportamental e Alerta dos servidores de diretórios de usuários Microsoft Active Directory, e deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios de dados;

**II.2.7.2** A solução deve possuir visibilidade da hierarquia do serviço de Diretórios através de interface gráfica e em formato de relatório;

**II.2.7.3** A solução deve possuir a visibilidade de todos os domínios, Unidades Organizacionais, Computadores, Grupos e outros objetos de domínio através de uma única interface gráfica e também em formato de relatório;

**II.2.7.4** A solução deve 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;

**II.2.7.5** A solução deverá ser capaz rastrear quem fez alterações no Active Directory, qual foi a alteração feita e quando nesta mesma interface gráfica e em formato de relatório;

**II.2.7.6** A solução deverá indicar de forma automática recomendações sobre grupos de segurança não utilizados e membros de grupos em sua interface gráfica e em forma de relatório;

**II.2.7.7** A solução deverá realizar a modelagem de permissionamento através de simulações de mudança para grupos e ACLs sem afetar o ambiente de produção, e identificando quais membros que efetivamente acessam os dados serão afetados,



permitindo a visibilidade anterior à realização das alterações no permissionamento de qual o impacto real no ambiente de produção;

## **II.2.8. Microsoft Exchange Server**

**II.2.8.1** A solução deve efetuar as funcionalidades de Permissionamento, Log, Relatórios, Análise Comportamental e Alerta dos servidores de correio eletrônico Microsoft Exchange, e deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios de dados;

**II.2.8.2** A solução ofertada deverá monitorar as caixas postais dos usuários, e as pastas compartilhadas deste servidor;

**II.2.8.3** A ferramenta deverá realizar a coleta das informações sem a oneração excessiva do servidor de correio Microsoft Exchange, ou seja, sem ativação do journaling ou diagnostics nativos do servidor de correio;

**II.2.8.4** As funcionalidades de análise comportamental deverão ser realizada dentro das pastas compartilhadas e caixas de correios dos servidores Microsoft Exchange monitorados;

**II.2.8.5** A ferramenta ofertada deverá coletar os eventos dos servidores de email monitorados contemplando no mínimo os seguintes itens:

- (a). Mensagem aberta;
- (b). Mensagem enviada;
- (c). Mensagem enviada “como” (on behalf of);
- (d). Mensagem enviada “em nome de”;
- (e). Mensagem editada;
- (f). Mensagem apagada;
- (g). Mensagem movida / copiada;
- (h). Mensagem marcada como lida / não lida;
- (i). Definição de sinalizadores;
- (j). Pasta aberta;
- (k). Pasta criada / apagada;
- (l). Permissões adicionadas / removidas / alteradas;
- (m). Pasta movida / copiada;
- (n). Anexo aberto;
- (o). Anexo apagado / adicionado;
- (p). Delegação de caixa de correio adicionada / removida;
- (q). Logon;

(r). Permissões de caixa de correio adicionadas / removidas;

### **II.2.9. Servidor de Arquivos Microsoft Windows**

**II.2.9.1** A solução deve efetuar as funcionalidades de Permissionamento, Log, Relatórios, Análise Comportamental e Alerta descrita nos itens acima em plataformas de servidores de arquivos Windows;

**II.2.9.2** A solução deve ter sua compatibilidade certificada em Windows 2003 e Windows 2008;

**II.2.9.3** Deverá suportar às tecnologias DAS, SAN, Windows-Powered NAS e suporte à tecnologia de cluster da Microsoft;

## **III – CONDIÇÕES DE ENTREGA E/OU FORNECIMENTO**

### **III.1. Locais da Entrega:**

**III.1.1.** FNDE: no SBS, Quadra 2, Bloco F, Edifício FNDE, Segundo Subsolo, CEP 70.070-929, Brasília-DF, na Coordenação-Geral de Infraestrutura Tecnológica;

### **III.2. Prazo de Entrega:**

**III.2.1.** Os serviços de fornecimento deverão ser executados **em até 90 (noventa) dias consecutivos a partir de ordem de serviço para fornecimento a ser emitida pelo FNDE** posterior à assinatura do contrato, e atendendo ao Cronograma de Execução abaixo:

#### **Cronograma de Execução:**

| <b>Fase</b> | <b>Descrição</b>                       | <b>Prazo em dias</b> |
|-------------|--|----------------------|
| 1           | Início do projeto                      | Em até D + 15        |
| 2           | Entrega dos produtos                   | Em até D + 30        |
| 3           | Planejamento e consultoria             | Em até D + 45        |
| 4           | Implementação e testes                 | Em até D + 75        |
| 5           | Transferência de conhecimentos         | Em até D + 90        |
| 6           | Documentação e Finalização do projeto  | Em até D + 90        |
| 7           | Manutenção e suporte técnico à solução | H + 36 meses         |

- Onde: D = data da emissão da **ordem de serviço para fornecimento**;
- Onde: H = data de emissão do **“Termo de Homologação”**

**III.2.2.** Contado da data da emissão do **“Termo de Homologação”**, deverão ser prestados os serviços de manutenção e suporte técnico pelo período de **36 (trinta e seis) meses**;

### **III.3. Forma de Fornecimento:**

**III.3.1.1** O fornecimento **deve ser executado de forma global**;

**III.3.1.2** Todo o fornecimento deve estar de acordo com os critérios estabelecidos nos itens deste Termo de Referência e em seus Encartes;

#### **IV – CONDIÇÕES DE RECEBIMENTO E PAGAMENTO**

##### **IV.1. Do Recebimento**

**IV.1.1.** O objeto deste Termo de Referência será dado como recebido de acordo com os artigos 73 a 76 da Lei 8.666/93, conforme:

**IV.1.1.1 Provisoriamente**, para efeito de posterior verificação de sua conformidade;

**IV.1.1.2 Definitivamente**, em **até 07 (sete) dias úteis**, a partir do devido atesto do Fiscal do Contrato e após minuciosa verificação e avaliação dos produtos e serviços fornecidos;

**IV.1.2.** O recebimento ocorrerá de acordo com os seguintes critérios:

| <b>Item</b>   | <b>Métrica</b> | <b>Indicador</b>              | <b>Valor</b>   |
|---|----------------|-------------------------------|----------------|
| Fornecimento de todo o software, com garantia       | Conjunto       | Softwares previstos entregues | 100% entregue  |
| Serviços profissionais (planejamento e consultoria) | Projeto        | Serviço executado             | 100% executado |
| Serviços profissionais (implementação e testes)     | Projeto        | Serviço executado             | 100% executado |
| Serviços de transferência de conhecimentos          | Projeto        | Serviço executado             | 100% executado |

**IV.1.3.** Para aceite do recebimento e posterior encaminhamento ao pagamento, deverão ser apresentados os seguintes documentos:

| <b>Item</b>   | <b>Documentos</b>   |
|---|---|
| Fornecimento de todo o software                     | Termo de Entrega<br>Tabela de Licenças                        |
| Serviços profissionais (planejamento e consultoria) | Termo de Aceite de Serviços de Planejamento e Consultoria     |
| Serviços profissionais (implementação e testes)     | Termo de Aceite de Serviços de Implementação e Testes         |
| Serviços de transferência de conhecimentos          | Termo de Aceite de Serviços de Transferência de Conhecimentos |

**IV.1.4.** Na conclusão de todos os serviços, a Contratada deverá apresentar “**Termo de Aceitação de Objeto**”, informando do encerramento de seus serviços e para atesto da entrega;

**IV.1.5.** O Fiscal do Contrato, de posse do “**Termo de Aceitação de Objeto**” apresentado pela Contratada e de toda a “**Documentação do Projeto**” (Encarte A), e após minuciosa verificação e avaliação dos produtos e serviços fornecidos, efetuará a emissão do competente “**Termo de Homologação**”;

**IV.1.6.** Independentemente da aceitação no recebimento, a Contratada deverá garantir a qualidade do serviço e produtos fornecidos pelo prazo estabelecido nas especificações e nas condições constantes deste Termo de Referência; obrigando-se a corrigir aquele que apresentar erro ou defeito, no prazo estabelecido pelo Contratante.

## **V – MOTIVAÇÃO**

**V.1.** Segundo o instituto de pesquisas técnicas e análises de tendências de TI – o GARTNER GROUP, cerca de **80% dos dados estratégicos** estão armazenados em *base de dados não estruturadas* ou *semi-estruturadas*. Esses dados estão distribuídos em pastas (departamentais, setoriais e individuais), acessadas entre os diversos Usuários de Rede e gerenciadas por Sistemas Operacionais que proporcionam o registro de eventos (LOG’S).

**V.2.** Apesar dos eventos registrados por Sistemas Operacionais, como Microsoft Windows, o respectivo acionamento para gravação requer recursos de memória e espaço em disco, incompatíveis com a capacidade operacional dos parques computacionais.

**V.3.** Além disto, uma vez registrados, a busca por informação desses eventos em nos “LOGs” é lenta, com interface ineficiente para consultas e pesquisas, além de não fazer monitoramento e análise crítica de eventos visando detecção antecipada de situações indevidas, tornando inviável qualquer tipo de gerenciamento e a auditoria de acesso a dados de forma real e imediata, sem geração de tráfego de rede.

**V.4.** Ou seja, com as ferramentas básicas que um Analista de SO ou Administrador de Rede possui é praticamente impossível **auditar quem acessou, modificou, apagou, renomeou ou enviou qualquer arquivo da base não estruturada**.

**V.5.** A base de dados do Microsoft Active Directory (AD) contém todas as informações sobre contas de usuários no ambiente Microsoft Windows, informações de correio eletrônico Microsoft Exchange Server, grupos de acessos às pastas dos servidores de arquivos, contas de computadores, dentre outros.

**V.6.** Desta forma, o serviço do AD armazena informações sobre objetos em uma rede e disponibiliza essas informações aos Analistas e Administradores da TI, proporcionando um modo de exibição intuitivo e hierárquico da sua estrutura de usuários, mas, no entanto, sua usabilidade em nível operacional somente atende às atividades básicas e diárias desses Analistas e Administradores, ficando diversas questões relacionadas à

**segurança de acesso, gerenciamento e monitoramento de eventos sensíveis e auditoria sem o devido suporte.**

**V.7.** O volume de usuários na rede interna do FNDE – aproximadamente 2000 (dois mil), torna atividade de “missão inexecutável” para os Analistas e Administradores da TI auditoria, controle e gerência de permissionamento dos serviços de AD (Microsoft Active Directory), servidor de Arquivos (Microsoft File Server) e sistema de correio eletrônico (Microsoft Exchange Server), especialmente de forma integrada.

**V.8.** São desafios que hoje esses Analistas e Administradores da TI enfrentam:

**V.8.1.** Identificar/classificar conteúdo sensível:

**IV.8.1.1** Pesquisar através de tantos dados demora muito;

**IV.8.1.2** Os dados mudam constantemente– difícil de manter a classificação atual;

**IV.8.1.3** Os resultados fornecem apenas o primeiro passo na proteção dos dados;

**V.8.2.** Identificar os proprietários dos dados:

**IV.8.2.1** Os metadados e os locais das pastas não fornecem a propriedade;

**IV.8.2.2** Muito tempo e processo manual para encontrar os donos;

**IV.8.2.3** Montantes significativos de dados “órfãos”–contexto de negócios ou relevância desconhecidos, espaço de armazenagem desperdiçado;

**V.8.3.** Entender QUEM acessou os dados e COMO:

**IV.8.3.1** A auditoria nativa prejudica a desempenho do servidor, gera grandes volumes de dados difíceis de decifrar;

**IV.8.3.2** A trilha de auditoria é habilitada somente depois de o incidente ter ocorrido;

**IV.8.3.3** A maioria não tem qualquer informação de auditoria;

**V.8.4.** Assegurar que as autorizações são baseadas em necessidades de negócios:

**IV.8.4.1** Como existem muitas mudanças, as autorizações crescem sempre;

**IV.8.4.2** As permissões raramente são negadas;

**IV.8.4.3** As ferramentas normalmente são manuais: demorado e sujeito a erros;

**V.9.** Com a presente contratação, pretende-se, portanto, superar os desafios acima relacionados e obter meios que permitam aos Analistas e Administradores da TI:

**V.9.1.** Visão completa da estrutura do AD, devendo ser possível administrar seu repositório de usuários e grupos de segurança através de uma interface única, juntamente com a gestão de seus servidores de arquivos;

**V.9.2.** Auditoria eficiente do Active Directory e Exchange, que por meio dos logs de auditoria você tem visibilidade de todos os eventos ocorridos;

**V.9.3.** Gestão do permissionamento e dos logs de todas as plataformas monitoradas em uma única console;

**V.9.4.** Relatórios visando facilitar o controle sobre o que acontece em todos os ambientes;

**V.9.5.** Alertas de modificação, quando alguma ação for disparada;

**V.9.6.** Consultas e pesquisas de eventos;

**ENCARTE C – Condições de manutenção e suporte técnico**

1. **Manutenção e assistência técnica do tipo corretiva**, compreendendo: procedimentos destinados à recolocar em perfeito estado de operação os serviços e softwares tais como:

1.1. Do software (aplicativos e sistema operacional): desinstalação, reconfiguração ou reinstalação decorrentes de falhas no software, atualização da versão de software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

1.1.1. Quanto às atualizações pertinentes aos softwares, entende-se como “atualização” o provimento de toda e qualquer evolução de software, incluindo correções, “patches”, “fixes”, “updates”, “service packs”, novas “releases”, “versions”, “builds”, “upgrades”, englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de manutenção e suporte técnico especificado;

1.2. A manutenção e assistência técnica corretiva serão realizadas sempre que solicitada pela Contratante por meio da abertura de chamado técnico diretamente à empresa Contratada (ou a sua Credenciada) via telefone (com número do tipo “0800” caso a Central de Atendimento esteja fora de Brasília-DF), Internet, e-mail ou fac-símile;

1.2.1. No atendimento aos chamados técnicos abertos, deverá ser disponibilizado **suporte personalizado** por um **Analista** designado;

1.2.2. Um chamado técnico somente poderá ser fechado após confirmação de responsável da Contratante e o término de atendimento se dará com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde o mesmo está instalado;

1.2.3. A prioridade de atendimento dos chamados será definida pela Contratante;

1.2.4. Na abertura de chamados técnicos, serão fornecidas informações, como Anormalidade observada, Nome do responsável pela solicitação do serviço e Versão do software utilizada no hardware e Severidade do chamado (ver tabela abaixo para cada tipo de produto);

| <b>TABELA DE SEVERIDADE DE CHAMADO</b> |  |                                       |
|--|--|---------------------------------------|
| <b>Severidade</b>                      | <b>Descrição</b>   | <b>Tempo de início de atendimento</b> |
| 1 – Urgente                            | Serviço parado no ambiente de produção                             | Em até 02 (duas) horas                |
| 2 – Muito Importante                   | Erros ou problemas recorrentes que impactam o ambiente de produção | Em até 04 (quatro) horas              |
| 3 – Importante                         | Problemas contornáveis   | Em até 08 (oito) horas                |
| 4 – Informação                         | Consulta técnica, dúvidas em geral,                                | Em até 12 (doze) horas                |

monitoramento, dentre outros.

1.2.5. Todas as solicitações feitas pelo FNDE deverão ser registradas pela Contratada em sistema informatizado para acompanhamento e controle da execução dos serviços e ainda:

- A Contratada após a realização dos serviços de manutenção e suporte técnico deverá apresentar um **Relatório de Visita**, contendo identificação do chamado, data e hora de abertura do chamado, data e hora do início e término do atendimento, identificação do defeito, técnico responsável pela solução, as providências adotadas e outras informações pertinentes. Este relatório deverá ser homologado por responsável do FNDE;

1.2.6. O tempo do início de atendimento do chamado técnico deverá ser de acordo com a Tabela de Severidade de Chamado e contado a partir da hora de abertura do chamado. Ou seja, a partir da hora de abertura do chamado, iniciada a contagem de tempo para o início do atendimento;

1.2.7. Em caso de necessidade e em qualquer classificação de severidade, a critério do FNDE, deverá ser prestado atendimento “On-Site”. Os serviços “On-Site” deverão iniciar-se em no máximo **02 (duas) horas** após confirmação do FNDE ou conforme agendamento a critério do órgão;

1.2.8. Após o início do atendimento, o tempo de solução do problema deverá ser de acordo com a Tabela de Solução do Chamado (ver tabela abaixo para qualquer tipo de produto), não devendo ultrapassar os prazos estabelecidos para as respectivas severidades, contados a partir da abertura do chamado técnico;

| <b>TABELA DE SOLUÇÃO DO CHAMADO</b> |  |                                   |
|-------------------------------------|--|-----------------------------------|
| <b>Severidade</b>                   | <b>Descrição</b>   | <b>Tempo de solução</b>           |
| 1 – Urgente                         | Serviço parado no ambiente de produção, incluindo reposição de peça defeituosa | Em até 04 (quatro) horas          |
| 2 – Muito Importante                | Erros ou problemas reincidentes que impactam o ambiente de produção            | Em até 08 (oito) horas            |
| 3 – Importante                      | Problemas contornáveis   | Em até 12 (doze) horas            |
| 4 – Informação                      | Consulta técnica, dúvidas em geral, monitoramento, dentre outros.              | Em até 48 (quarenta e oito) horas |

1.2.9. Um chamado somente poderá ser fechado após confirmação de responsável do FNDE e o término de atendimento se dará com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde o mesmo está instalado;

1.2.10. A Contratada será eximida da aplicação das sanções administrativas para os respectivos chamados em que sejam descumpridos os tempos de solução, desde que comprovadas as seguintes situações:



- Quando constatado que o problema está relacionado a "bug" no produto e que o fabricante não possui uma correção imediata para tal, sendo este fato declarado pelo próprio; e
- Que a Contratada tomou todas as medidas possíveis visando providenciar solução de contorno;

1.3. Este serviço deve estar disponível para **acionamento e atendimento** no sistema **7 x 24 (sete dias na semana, vinte e quatro horas por dia)**;

## 2. **Suporte técnico para acompanhamento dos serviços**, compreendendo:

2.1. Para o acompanhamento dos serviços desta contratação, a Contratada deverá disponibilizar equipe de Suporte Técnico contemplando no mínimo um Gerente de Suporte, além de Técnicos Especialistas necessários aos serviços, os quais deverão ser profissionais capacitados e certificados nos produtos objeto deste Termo de Referência;

2.2. Este Gerente de Suporte ficará responsável pelo acompanhamento dos serviços de manutenção e assistência técnica (tanto corretiva quanto preventiva) e de toda e qualquer demanda apresentada pela Contratante objeto dos serviços;

2.3. O Gerente de Suporte também será o responsável por elaborar qualquer documentação técnica relativa aos serviços, incluindo um Plano de Suporte Técnico mensal e anual;

3. O FNDE poderá **utilizar** os softwares em locais **fora de suas dependências**, sem prejuízo das condições de manutenção e suporte técnico previstas neste Termo de Referência, desde que:

3.1. Efetue comunicação prévia à Contratante da mudança dos novos locais de residência dos recursos;

3.2. Os novos locais de residência deverão ter instalações físicas dentro das normas e padrões específicas, e que tenham sido informadas previamente à Contratada, a qual decidirá por uma visita ao local para vistoria;

3.3. Caso os novos locais de residência estejam fora da localidade de Brasília-DF, a Contratada deverá informar os adicionais de custo nos valores dos serviços para atendimento, bem como dos tempos adicionais aos prazos de atendimento;

4. A Contratada deverá informar aos responsáveis da Contratante qualquer situação que possa ensejar em uso inadequado dos recursos;

4.1. A Contratada será eximida de despesas de manutenção e suporte técnico decorrentes uso inadequado dos recursos, desde que devidamente comprovadas;

5. A Contratada não poderá deixar de executar os serviços descritos neste Encarte sob qualquer alegação, mesmo sob pretexto de não ter sido executada anteriormente qualquer tipo de interferência no respectivo produto ou dispositivo;
6. Para os serviços descritos neste Encarte, o FNDE permitirá o acesso dos técnicos habilitados e identificados da Contratada às instalações onde se encontrarem os produtos. Esses técnicos ficarão sujeitos a todas as normas internas de segurança do FNDE, inclusive àquelas referentes à identificação, trajes, trânsito e permanência em suas dependências;
7. Para a execução dos serviços descritos neste Encarte, a Contratada somente poderá desativar o produto, com prévia autorização do FNDE;