PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

CONTRATO N. 034/2015 – CJF

PROCESSO N. CJF-ADM-2015/00201

ADESÃO ATA DE REGISTRO DE PREÇOS N. 1/2015 - EMBRATUR

DADOS DA EMPRESA
CONTRATADA: VERT SOLUÇÕES EM INFORMÁTICA LTDA
CNPJ/MF: 02.277.205/0001-44
ENDEREÇO: SHS, Quadra 06, Conjunto A, Bloco A, Salas 403 e 404, Asa Sul, Brasília - DF
TELEFONE: (61) 9249-9286 (61) 2103-1006 (Sérgio Mamede)
E-MAIL: sergio.mamede@vert.com.br; priscila.silva@vert.com.br
SIGNATÁRIO CONTRATADA: HIRAN RICARDO FRANCO DA SILVA – Vice-Presidente
SIGNATÁRIO CJF: EVA MARIA FERREIRA BARROS - Diretora - Geral

DADOS DO CONTRATO
OBJETO: Aquisição de solução baseada em software totalmente compatível com ambiente Microsoft e servidor de arquivos UNIX, para implantação de auditoria, controle e gerência de permissionamento dos serviços de diretório (Microsoft Active Directory), servidor de arquivos (Microsoft File Server), servidor de colaboração SharePoint (Microsoft Sharepoint Server), Servidor de Arquivos UNIX/Linux e Correio Eletrônico (Microsoft Exchange Server).
FUNDAMENTAÇÃO LEGAL: Lei n. 10.520, de 17 de julho de 2002, os Decretos n. 2.271, de 07 de julho de 1997, e 5.450, de 31 de maio de 2005, e a Lei n. 8.666, de 21 de junho de 1993, Instrução Normativa n. 02, de 30 de abril de 2008 e Instrução Normativa n. 04, de 12 de novembro de 2010 e posteriores alterações, bem como as demais normas e regulamentos aplicados à matéria.
VIGÊNCIA: 11/12/2015 a 10/12/2016
VALOR DO CONTRATO: R$ 551.609,00
UNIDADE FISCALIZADORA: STI

PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

CONTRATO N. 034/2015 – CJF

Contrato que entre si celebram, o **CONSELHO DA JUSTIÇA FEDERAL** e a empresa **VERT SOLUÇÕES EM INFORMÁTICA LTDA**, para aquisição de solução baseada em *software* totalmente compatível com ambiente *Microsoft* e servidor de arquivos UNIX.

CONTRATANTE: **UNIÃO,** por intermédio do **CONSELHO DA JUSTIÇA FEDERAL,** Órgão integrante do Poder Judiciário, inscrito no CNPJ/MF n. 00.508.903/0001-88, com sede no Setor de Clubes Esportivos Sul, Trecho III, Polo 8, Lote 9, Brasília-DF, neste ato representado por sua Diretora - Geral, a Senhora **EVA MARIA FERREIRA BARROS,** brasileira, inscrita no CPF/MF n. 188.490.083-68, portadora da Carteira de Identidade n. 666.351-SSP/DF, residente e domiciliada em Brasília - DF.

CONTRATADA: **VERT SOLUÇÕES EM INFORMÁTICA LTDA**, inscrita no CNPJ/MF n. 02.277.205/0001-44, estabelecida no SHS, Quadra 06, Conjunto A, Bloco A, Salas 403 e 404, Asa Sul, Brasília - DF, neste ato representada pelo Vice-Presidente, o Senhor **HIRAN RICARDO FRANCO DA SILVA**, brasileiro, inscrito no CPF/MF n. 287.734.891-15, portador da Carteira de Identidade n. 651942-SSP/DF e CNH n. 02814676127 – DETRAN/DF, residente e domiciliado em Brasília - DF.

Consoante o Processo n. CJF-ADM-2015/00201 e, em observância ao disposto na Lei n. 10.520, de 17 de julho de 2002, os Decretos n. 2.271, de 07 de julho de 1997, e 5.450, de 31 de maio de 2005, e a Lei n. 8.666, de 21 de junho de 1993, Instrução Normativa n. 02, de 30 de abril de 2008 e Instrução Normativa n. 04, de 12 de novembro de 2010 e posteriores alterações, bem como as demais normas e regulamentos aplicados à matéria, resolvem celebrar o presente Contrato, sob os termos e condições estabelecidos nas cláusulas adiante.

1. DO OBJETO

1.1 - Aquisição de solução baseada em software totalmente compatível com ambiente Microsoft e servidor de arquivos UNIX, para implantação de auditoria, controle e gerência de permissionamento dos serviços de diretório (Microsoft Active Directory),

servidor de arquivos (Microsoft File Server), servidor de colaboração SharePoint (Microsoft Sharepoint Server), Servidor de Arquivos UNIX/Linux e Correio Eletrônico (Microsoft Exchange Server) do CONTRATANTE, bem como execução de serviços de planejamento, consultoria, implementação e testes, além de transferência de conhecimentos, com garantia (manutenção e suporte técnico) pelo período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste Contrato.

1.2 - Vinculam-se ao presente Contrato o Edital de Pregão n. 17/2014 com seus anexos, proposta da CONTRATADA e demais documentos que compõem o processo em referência, independentemente de transcrição.

2. ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO

2.1 - Objetiva-se com a contratação efetuar a implantação de uma solução de auditoria, controle e gerência de permissionamento dos serviços de diretório (Microsoft Active Directory, LDAP e NIS), servidor de arquivos (Microsoft File Server), servidor de colaboração SharePoint (Microsoft Sharepoint Server), Servidor de Arquivos UNIX/Linux e Correio Eletrônico (Microsoft Exchange Server), os quais são responsáveis pela comunicação e armazenamento dos dados não estruturados do ÓRGÃO, contemplando:

2.1.1 - Licenciamento completo de até 500 usuários internos

2.1.2 - Execução de serviços profissionais para implementação e testes, para até 500 usuários, possibilitando a aquisição dos serviços em lotes de até 500 usuários internos, de acordo com o item 2.1.

2.1.3 - Instalação e configuração da solução (softwares) no ambiente da CONTRATANTE;

2.1.4 - Integração e compartilhamento de recursos e auditoria, controle, gerenciamento e permissionamento da solução com o ambiente de produção existente;

2.1.5 - Execução de serviços profissionais de até 1.000 horas de consultoria para customização e ajustes dos itens adquirido no item 2.1, a serem executados dentro do prazo vigente do contrato;

2.1.6 - Transferência de conhecimentos composta por turmas de 3 alunos, possibilitando a aquisição de até 5 turmas na modalidade de ata de registro de preços;

2.1.7 - Serviço de manutenção e suporte pelo período de 36 (trinta e seis) meses;

2.2 - Descrição detalhada da solução

2.2.1 - Características funcionais:

2.2.1.1 - A solução ofertada deverá reter as informações de log e histórico em banco de dados (MS SQL ou Oracle), seja ele na máquina local ou em SQL Farm já existente dentro do ÓRGÃO por um período que será determinado na fase de escopo do projeto (mínimo de 12 meses);

2.2.1.2 - As licenças do ambiente operacional para instalação do produto, incluindo o Sistema Operacional e o banco de dados para a solução serão fornecidos pela CONTRATANTE;

2.2.1.3 - 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;

2.2.1.4 - A solução deverá contemplar na mesma console a possibilidade de englobar as funcionalidades através de agentes adicionais para no mínimo as plataformas, Microsoft Active Directory, LDAP, NIS, Microsoft Exchange Server, Microsoft Sharepoint Server e Windows Server e UNIX Servers;

2.2.1.5 - Caso a solução utilize um agente nos servidores a serem monitorados, sua instalação não deve requerer a reinicialização dos mesmos;

2.2.1.6 - 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;

2.2.1.7 - 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;

2.2.1.8 - A solução deve fornecer método para assinalar ou associar um usuário como "Proprietário" de uma pasta ou grupo;

2.2.1.9 - 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;

2.2.1.10 - Deve permitir o gerenciamento das funcionalidades através de console própria ou por navegador WEB;

2.2.1.11 - Fornecer interface única de usuário para exibir as permissões, os detalhes da auditoria, as estatísticas de acesso a dados e alertas;

2.2.1.12 - A solução deve suportar a utilização de servidores Virtualizados (VMWare) para todos os seus componentes;

2.2.1.13 - A solução deve contemplar o licenciamento dos bancos de dados e sistemas operacionais para a instalação e monitoração da solução;

2.3 - Controle de acessos (permissionamento)

2.3.1 - 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.

2.3.2 - 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, subgrupos e seus respectivos membros.

2.3.3 - 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.

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

2.3.5 - A ferramenta deverá prover filtros para visualizar todos os objetos de dados de forma gráfica incluindo pastas protegidas e únicas.

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

2.3.6 - A ferramenta não deve restringir a quantidade das listas de acesso (ACLs) coletadas e/ou armazenadas.

2.3.7 - A visualização de grupos deve compreender todos os grupos filhos (subgrupos) sem restrição de número de hierarquias.

2.3.8 - A solução deve possibilitar a configuração de uma credencial diferente para cada volume a ser monitorado.

2.3.9 - 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.

2.3.10 - 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.

2.3.11 - 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.

2.3.12 - 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.

2.4 - Registro de eventos (log)

2.4.1 - A solução deve coletar o log de forma normatizada dos repositórios de dados em plataforma Serviço de Diretórios, Servidores de Arquivos Windows e UNIX/LINUX, Sharepoint e Microsoft Exchange.

2.4.2 - A solução ofertada deve manter o log das operações de abrir, criar, apagar, modificar, copiar, renomear e acesso negado.

2.4.3 - 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.

2.4.4 - Deverá permitir filtragem gráfica, ordenação e agrupamento dos logs.

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.

2.4.5 - Fornecer resumo gráfico das atividades auditadas, incluindo:

2.4.6 - Visualização dos usuários mais e menos ativos;

2.4.7 - Visualização dos diretórios mais e menos ativos;

2.4.8 - Visualização dos diretórios onde um usuário ou um grupo de usuários estejam acessando;

2.4.9 - Visualização dos usuários que estejam acessando um diretório;

2.4.10 - A ferramenta deve normatizar eventos relacionados e apresentar como um único evento para o mesmo objeto;

2.4.11 - A solução deve permitir auditoria direta de quem tem acesso aos dados na tela da console, sem necessidade de gerar relatório demonstrativo.

2.5 - Relatórios

2.5.1 - A solução ofertada deve gerar relatórios nos formatos TXT, CSV, HTML, XLS e PDF.

2.5.2 - A ferramenta deve permitir o agendamento para envio de relatórios pelo correio eletrônico.

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

2.5.4 - 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.

2.5.5 - A ferramenta deve possibilitar a definição da prioridade de cada relatório agendado.

2.5.6 - A ferramenta deve fornecer relatórios customizáveis sob demanda e agendados.

2.5.7 - A ferramenta deve fornecer relatório dos acessos aos arquivos.

2.5.8 - A ferramenta deve armazenar todas as modificações feitas nas permissões dentro e fora da interface gráfica.

2.5.9 - Fornecer relatórios sobre onde a permissões concedidas a grupos globais (Everyone, Domain Users, Users) estão sendo utilizadas.

2.5.10 - Armazenar todas as modificações em grupos feitas dentro e fora da interface gráfica.

2.5.11 - Fornecer relatórios de grupos de segurança vazios ou não utilizados.

2.5.12 - Fornecer relatórios de SIDs não resolvidos e usuários com permissão direta em pastas.

2.5.13 - Fornecer relatórios de dados e usuários inativos.

2.5.14 - Fornecer relatórios sobre administradores acessando dados de negócio.

2.5.15 - Fornecer relatórios de usuários desabilitados que ainda fazem parte de grupos de segurança.

2.5.16 - 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.

2.5.17 - Possibilitar o direito de revisão de gestão de dados através de relatórios indicativos do uso dos dados.

2.5.18 - Suprir com rotinas automatizadas, relatórios programados e outras facilidades sobre os benefícios esperados, destes relatórios.

2.5.19 - A solução deve ser capaz de fornecer relatórios para auditoria e conformidade (compliance).

2.6 - Analise Comportamental

2.6.1 - 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.

2.6.2 - A solução deve identificar, de forma automática, usuários com acesso a pastas e\ou arquivos indevidos sugerindo a revogação de acesso.

2.6.3 - A solução deverá fornecer em modo gráfico recomendações sobre permissionamento excessivo, baseado na análise de atividade de acesso.

2.6.4 - Fornecer identificação gráfica de atividades de acesso anormais.

2.6.5 - Estas recomendações deverão também ser fornecidas em forma de relatório.

2.7 - Sistema de notificações (alertas)

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

2.7.2 - A notificação deverá ser feita também via e-mail.

2.7.3 - A ferramenta deve emitir um alerta quando um usuário desviar do seu comportamento padrão.

2.7.4 - Fornecer relatórios sobre atividades de acesso anormais.

2.8 - Módulo Permissionamento de Serviços Active Directory (AD)

2.8.1 - A solução deve efetuar as funcionalidades de Permissionamento, Log, Relatórios, Alertas dos serviços de diretórios de usuários como Microsoft Active Directory, LDAP, NIS e usuários locais dos servidores, e deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios de dados.

2.8.2 - A solução deve possuir visibilidade da hierarquia dos Serviços de Diretórios dos Usuários através de interface gráfica e em formato de relatório.

2.8.3 - Solução deve possuir visibilidade da hierarquia dos Serviços de Diretórios dos Usuários através de interface gráfica e em formato de relatório.

2.8.4 - A solução deve ter trilha de auditoria classificável e pesquisável de todas as atividades do Active Directory, LDAP, NIS e usuários locais dos servidores em uma única interface gráfica e também em formato de relatório.

2.8.5 - Solução deverá ser capaz rastrear quem fez alterações no Active Directory, LDAP, NIS e usuários locais dos servidores, qual foi a alteração feita e quando, nesta mesma interface gráfica e em formato de relatório.

2.8.6 - 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.

2.8.7 - 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, permitindo a visibilidade anterior à realização das alterações no permissionamento de qual o impacto real no ambiente de produção.

2.8.8 - A solução ofertada deverá suportar o gerenciamento do Microsoft Active Directory ao ponto de permitir os administradores da solução no mínimo as seguintes funcionalidades:

2.8.8.1 - Criação de novos usuários;

2.8.8.2 - Criação de novos grupos;

2.8.8.3 - Alteração de parâmetros de usuários já existentes;

2.8.8.4 - Deleção de usuários;

2.8.8.5 - Deleção de computadores;

2.8.8.6 - Reset de senhas;

2.8.8.7 - Desbloqueio de usuários;

2.8.8.8 - Desabilitação de usuários;

2.8.8.9 - A solução deverá ser compatível, no mínimo, com as versões do Microsoft AD 2003, 2008 e 2012.

2.9 - Módulo Microsoft Exchanger Server

2.9.1 - 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.

2.9.2 - A solução ofertada deverá monitorar as caixas postais dos usuários, e as pastas compartilhadas deste servidor.

2.9.3 - 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.

2.9.4 - Caso a solução necessite a ativação do Journaling do Exchange deverá ser fornecido o hardware necessário para o armazenamento deste journaling por 12 (doze) meses.

2.9.5 - As funcionalidades de análise comportamental deverão ser realizadas dentro das pastas compartilhadas e caixas de correios dos servidores Microsoft Exchange monitorados.

2.9.6 - A ferramenta ofertada deverá coletar os eventos dos servidores de e-mail monitorados contemplando no mínimo os seguintes itens:

2.9.6.1 - Mensagem aberta;

2.9.6.2 - Mensagem enviada;

2.9.6.3 - Mensagem enviada "como" (on behalf of);

2.9.6.4 - Mensagem enviada "em nome de";

2.9.6.5 - Mensagem editada;

2.9.6.6 - Mensagem apagada;

2.9.6.7 - Mensagem movida / copiada;

2.9.6.8 - Mensagem marcada como lida / não lida;

2.9.6.9 - Definição de sinalizadores;

2.9.6.10 - Pasta aberta;

2.9.6.11 - Pasta criada / apagada;

2.9.6.12 - Permissões adicionadas / removidas / alteradas;

2.9.6.13 - Pasta movida / copiada;

2.9.6.14 - Anexo aberto;

2.9.6.15 - Anexo apagado / adicionado;

2.9.6.16 - Delegação de caixa de correio adicionada / removida;

2.9.6.17 - Logon;

2.9.6.18 - Permissões de caixa de correio adicionadas / removidas.

2.9.7 - A solução deverá auditar, registrar eventos (log) e aplicar as análises comportamentais das caixas postais e pastas compartilhadas do Microsoft Exchange Server para eventos gerados a partir de dispositivos moveis e/ou acessos externos (via internet) por meio de acesso WEB através dos seguintes protocolos de comunicação contemplando no mínimo os seguintes itens:

2.9.7.1 - POP3 – Post Office Protocol v3;

2.9.7.2 - IMAP – Internet Message Access Protocol;

2.9.7.3 - MAPI - Messaging Application Programming Interface;

2.9.7.4 - OWA – Outlook Web Access;

2.9.7.5 - EWS – Exchange Web Services;

2.9.7.6 - ActiveSync - para smartphones e outros dispositivos similares.

2.9.8 - A solução deverá registrar eventos (logs) contendo informações do IP de origem do dispositivo móvel ou computador de onde foi acessada a caixa postal.

A solução deve ser compatível com o Microsoft Exchange Server no mínimo nas versões 2007 e 2010.

2.10 - Módulo Microsoft Windows Server:

2.10.1 - 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.

2.10.2 - A solução deve ter sua compatibilidade certificada em Windows Server 2003, 2008 e 2012.

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

2.10.4 - Integrar com as plataformas de storage existentes VNX da EMC e NetAPP sem a necessidade de instalação de softwares ou agentes.

2.11 - Módulo Microsoft Sharepoint Server:

2.11.1 - A solução deve efetuar as funcionalidades de permissionamento, Log, Relatórios, Análise Comportamental e Alerta descrita nos itens acima em plataformas de servidores de arquivos Microsoft Office Sharepoint Server:

2.11.2 - A solução deve ter sua compatibilidade certificada em Microsoft Office Sharepoint Server x64 e x86 para as plataformas 2007, 2010 e 2013;

2.12 - Módulo Microsoft UNIX Server:

2.12.1 - A solução deve efetuar as funcionalidades de Permissionamento, Log, Relatórios, Análise Comportamental e Alertas descritos nos itens acima em plataformas de servidores de arquivos LINUX.

2.12.2 - A solução deve ter sua compatibilidade certificada em no mínimo as seguintes versões:

2.12.2.1 - Red Hat 4 Kernel 2.6.9:

a. smp - 32 bit;
b. Hugemem - 32 bit;
c. smp - 64 bit;
d. LargeSmp - 64 bit.

2.12.2.2 - Red Hat 5 Kernel 2.6.18:

a. smp - 32 bit
b. xen–smp - 32 bit;
c. pae–smp - 32 bit;
d. smp - 64 bit

2.12.2.3 - Red Hat 6 Kernel 2.6.32:

a. smp - 32 bit;
b. smp - 64 bit

2.12.2.4 - SUSE SLES 10 Kernel 2.6.16:

a. xenpae-smp - 32 bit;
b. smp - 64 bit

2.12.2.5 - Ubuntu 8.04 LTS Kernel 2.6.24:

a. smp – 32 and 64 bit;

2.12.2.6 - Ubuntu 10.04 LTS Kernel 2.6.32-38:

a. smp - 64 bit;
b. pae-smp - 32 bit

2.13 - Módulo Portal de Permissionamento:

2.13.1 - A solução deverá permitir que os usuários donos das pastas permitam acesso aos seus dados não estruturados e semiestruturados a outros usuários, bem como a revogação destes acessos, sem necessidade de envolvimento do administrador do sistema;

2.13.2 - Ter interface web para solicitação de permissionamento/participação em grupo de segurança;

2.13.3 - Ser capaz de personalizar um fluxo de aprovação para cada demanda do usuário;

2.13.4 - Enviar e-mail de notificação ao aprovador/dono da informação quando uma nova solicitação for aberta a ele:

2.13.5 - Possibilitar a escolha de uma data de expiração/validade do permissionamento aprovado;

2.13.6 - Revogar automaticamente as permissões escolhidas na sua data de expiração sem que se faça necessária a intervenção de um usuário;

2.13.7 - Criar revisões de permissionamento direcionadas diretamente ao dono de cada pasta/grupo;

2.13.8 - Sinalizar nas revisões de permissionamento, quais usuários poderiam ter suas permissões removidas sem que haja impacto ao negócio;

2.13.9 - Disponibilizar para o responsável por cada conjunto de dados, acesso aos logs de auditoria, estatísticas e permissões;

2.13.10 - Permitir a criação de regras de segurança para que usuários ou grupos de usuários nunca tenham acesso a determinado conjunto de dados;

2.13.11 - Forçar as regras de segurança para que caso uma permissão seja concedida diretamente, o software as remova sem a intervenção de um usuário;

2.13.12 - A solução deverá prover a habilidade de identificar os proprietários dos dados e enviar aos mesmos relatórios sobre permissionamento e acesso.

2.14 - Módulo Migração de Dados Automatizados entre plataformas:

2.14.1 - A solução deve permitir a migração de dados entre plataformas no mínimo:

2.14.1.1 - CIFS para Sharepoint:

a. Deve permitir a personalização e simulação nas alterações de permissões antes da migração. (Ex.: a critério do administrador a permissão "Leitura" no CIFS se tornará "Contribuir" no Sharepoint, a permissão "Modificar" se tornará "Gerenciar Hierarquia", etc).

2.14.1.2 - Sharepoint para CIFS

2.14.2 - A solução deve permitir a migração de dados entre domínios:

2.14.2.1 - A solução deve permitir migrar mantendo as permissões, metadados e ACL's;

2.14.2.2 - A solução deve automaticamente, na migração entre domínios, criar novos grupos no active directory, mantendo assim as mesmas permissões de usuários que estavam no antigo repositório.

2.14.3 - A solução deve permitir configurar e programar o horário e com qual frequências as migrações irão ocorrer.

2.14.4 – A solução deve permitir migrar dados em horário de produção sem que haja interrupção ao usuário e perdas de dados;

2.14.5 - A solução deve permitir a migração dos dados com base nas recomendações sugeridas pela ferramenta de auditoria;

2.14.6 - A solução deve permitir migrar alterando as permissões de acordo com as recomendações;

2.14.7 - A solução deve permitir em interface gráfica simular o impacto da migração baseadas nas regras definidas;

2.14.8 - A solução deve permitir ao administrador, refinar e editar as permissões ACL's antes da migração;

2.14.9 - A solução deve ter a capacidade de simular os efeitos de permissão sobre os utilizadores pós-migração;

2.14.10 - A solução deve permitir deixar as permissões como estão ou torna-las melhor com base nas recomendações feitas pela solução de auditoria;

2.14.11 - A solução deve permitir migrações incrementais, baseadas somente nos dados novos ou alterados do primeiro repositório;

2.14.12 - A solução deve permitir migrar mantendo as mesmas estruturas de hierarquia de pastas no novo repositório;

2.14.13 - A solução deve ter a opção de migrar todo o conteúdo das pastas ou somente a estrutura de pastas;

2.14.14 - A solução deve possuir algoritmo para identificar e solucionar colisões em nomes de arquivos e pastas;

2.14.15 - A solução deve através de metadados e regras de classificação possibilitar a identificação de arquivos e pastas e migrar entre plataformas, domínios distintos, mantendo as permissões, metadados e ACL's;

Verr Soluções em TIC
Jurídico
PTM

2.14.16 - A solução deve permitir a identificação de dados não acessados por determinado período de tempo e migrar entre plataformas, domínios distintos, mantendo as permissões, metadados e ACL's;

2.14.17 - A solução deve em conjunto com a ferramenta de classificação possibilitar a migração de dados sensíveis entre plataformas, domínios distintos, mantendo as permissões, metadados e ACL's;

2.14.18 - A solução deve através de metadados possibilitar a identificação de arquivos por extensão, tamanho, nome, e migrar entre plataformas, domínios distintos, mantendo as permissões, metadados e ACL's;

2.14.19 - A solução deve através da ferramenta de auditoria possibilitar a identificação de mais usados e migrar entre plataformas, domínios distintos, mantendo as permissões, metadados e ACL's;

2.14.20 - A solução deve permitir criar regras de migração automática, continua e única, possibilitando assim que qualquer arquivo ou documento novo incluído no repositório de dados seja automaticamente migrado entre plataformas, domínios distintos, mantendo as permissões, metadados e ACL's;

2.14.21 - A solução deve permitir criar regras de migração automática, baseadas em regras de negócio, migrado entre plataformas, domínios distintos, mantendo as permissões, metadados e ACL's.

2.15 - Módulo Acesso de dados remotos:

2.15.1 - A solução deverá suportar o acesso simultâneo para as quantidades de usuário adquiridas, de acordo com o item 2.1.2.

2.15.2 - A solução ofertada deve permitir que os sistemas de arquivos, CIFS e NFS, atualmente implementados no ÓRGÃO seja compartilhados de maneira segura para os usuários externos e internos;

2.15.3 - A solução deverá realizar a função de proxy e streamline de acesso seguro (HTTPS) para a o servidor de arquivos já implementada com base nos protocolos NFS e CIFS;

2.15.4 - A comunicação entre a solução ofertada e repositório de usuário, para autenticação dos mesmos, se dará através do protocolo LDAP;

2.15.5 - A autenticação deve utilizar base de usuários dos diretórios de serviços corporativos, sendo compatíveis com bases LDAP v.3 e Microsoft Active Directory, sem a necessidade de criação de base interna para esta finalidade;

2.15.6 - A autenticação dos usuários deverá ocorrer através do protocolo HTTPS sem a necessidade de certificados digitais ou VPN;

2.15.7 - A sincronia de dados entre a solução e o cliente deverá ser realizada através do protocolo HTTPS;

2.15.8 - O cliente deve notificar os usuários para cada alteração feita nos arquivos;

2.15.9 - Solução deverá implementar a sincronia automática entre arquivos e pastas armazenados nos repositórios CIFS e NFS do ÓRGÃO e os clientes da solução, como

computadores, laptops, smartphones e tablets dos funcionários internos e externos de maneira segura. No mínimo para os seguintes clientes;

2.15.9.1 - Windows (Vista, 7 ou superior);

2.15.9.2 - Apple iOS (iPhone e iPad);

2.15.9.3 - Android;

2.15.10 - A solução deve possibilitar a adição de novos arquivos e arquivos editados, através de smartphones e tablets;

2.15.11 - A solução deve possibilitar o acesso aos compartilhamentos e arquivos através do navegador WEB;

2.15.12 - Os arquivos devem ser disponibilizados sem a utilização de serviços externos e utilização de cache a própria solução, devendo armazenar os arquivos estritamente nos repositórios internos e nos clientes autorizados para a solução;

2.15.13 - A sincronia entre os dispositivos deverá ocorrer sem que haja a necessidade de alocação de novos espaços, com a criação de novos arquivos ou pastas, nos repositórios atualmente em utilização;

2.15.14 - As permissões para acesso aos arquivos e pastas devem obedecer as mesmas regras definidas para a base de usuários existente, expressas no compartilhamento CIFS e NFS;

2.15.15 - Deve ser possível o fornecimento de links web para compartilhamento de arquivos, pastas e um espaço para upload de arquivos para colaboradores externos ao ÓRGÃO, desde que autorizado pelo administrador da rede.

2.15.16 - O acesso aos arquivos e diretórios realizados por colaboradores externos deve possuir dois modos de compartilhamentos, conforme descrito abaixo;

2.15.16.1 - Público: Permite o acesso aos dados por qualquer um que possua o link;

2.15.16.2 - Privado: O acesso será permitido somente ao usuário destinatário, através do uso de uma senha de identificação (pin) que será alterada em cada acesso realizado pelo colaborador externo;

2.15.17 - Para cada uma das pastas adicionadas ao serviço de compartilhamento e sincronia deve ser possível a definição do tipo de compartilhamento, com no mínimo as seguintes opções;

2.15.17.1 - Compartilhamento Externo;

2.15.17.2 - Compartilhamento Interno;

2.15.17.3 - Compartilhamento Externo e Interno;

2.15.18 - Deve permitir a definição de data de expiração para o compartilhamento das pastas e arquivos;

2.15.19 - A solução deverá fornecer uma pasta para upload para uso de colaboradores externos;

2.15.20 - A solução não deve restringir o tamanho dos arquivos compartilhados;

2.15.21 - A Pasta de upload deve permitir o controle de validade (tempo) e tamanho de arquivos;

2.15.22 - Solução deve emitir um alerta para o administrador informando que arquivos e pastas internas foram compartilhados com colaboradores externos;

2.15.23 - A Solução deverá controlar o acesso aos dados mantendo registro das operações de abrir, criar, apagar, modificar, copiar renomear e de acesso negado;

2.15.24 - Deverá implementar a coleta de log de forma normatizada dos repositórios de dados Windows e Linux;

2.16 - Módulo de Classificação de Dados sensíveis e integração com DLP

2.16.1 - A solução deve ser capaz de identificar qual dado ou arquivo contém informações sensíveis ou confidenciais.

2.16.2 - A solução deve identificar dados sensíveis nas plataformas Windows e NAS.

2.16.3 - A solução deve exibir na mesma interface gráfica informações sobre os permissionamentos, ACL's , quantidade de informações sensíveis e qual tipo de informação sensível classificada, a fim de facilitar a identificação de potenciais repositórios e pastas super expostos.

2.16.4 - A solução deve gerar em forma de relatórios dados sobre a classificação das informações.

2.16.5 - A solução deve ter a capacidade de Incluir filtros sobre a classificação dos dados nas pesquisas dos Logs.

2.16.6 - A solução deve ter a capacidade de Incluir filtros sobre a classificação dos dados nos relatórios de acesso.

2.16.7 - Para cada arquivo marcado como sensível, a solução deve possibilitar a visão, diretamente da ferramenta, das expressões regulares ou strings que fizeram com que esse arquivo fosse considerado como sensível.

2.16.8 - A solução deve fornecer visibilidade de conteúdo crítico de negócios através da classificação da informação.

2.16.9 - A ferramenta deve fornecer visibilidade dos locais que possuem dados sensíveis.

2.16.10 - A solução deve gerar recomendações acionáveis para redução de acesso aos dados classificados como sensíveis.

2.16.11 - A solução deve integrar a funcionalidade de classificação de dados sensíveis com soluções de terceiros para estender a habilidade de ambos.

2.16.12 - A solução deve possibilitar a instalação da funcionalidade de classificação de dados sensíveis em um único servidor, sem a necessidade de servidores adicionais.

2.16.13 - A solução deve fornecer a funcionalidade de busca de arquivos através de palavras-chave, frases e/ou expressões regulares.

2.16.14 - A ferramenta deve 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.

2.16.15 - A solução deve classificar dados utilizando mecanismo de busca próprio capaz de pesquisar conteúdos sensíveis através de "strings", expressões regulares ou regras pré-definidas;

2.16.16 - A solução deverá realizar uma busca dentro de arquivos word, excel, pdf, txt. dos conteúdos identificados como sensíveis e delimitados nas "strings"

2.16.17 - Deve ser possível priorizar a ordem pelas quais os arquivos sensíveis serão buscados, como por exemplo, filtrar primeiramente os mais acessados, os maiores, entre outros.

2.17 - Demais Componentes

2.17.1 - Todos os componentes passivos adicionais que se fizerem necessários para efetivar as interligações dos ativos do objeto da contratação;

2.17.2 - Visando preservar harmonia entre todos os elementos da solução, a total interoperabilidade de componentes e a facilidade de uso e operação, a solução fornecida deverá ser de um único fabricante em que seus módulos e ou programas sejam totalmente integrados e disponibilizados em uma única console de gerência;

2.17.3 - O modulo (esquema) de segurança da solução (software) não deverá implicar em aquisição de componentes (hardware e software) adicionais;

2.17.4 - Deverá ser compatível e permitir a utilização da tecnologia "hyperthreading" sem custos adicionais;

2.17.5 - A solução deverá possibilitar integração, de forma direta ou indireta, de suas informações com sistemas de DLP (Data Lost Prevention);

2.18 - Módulo Serviços profissionais para implementação e testes

2.18.1 - Execução de todos os serviços profissionais para Implementação e Testes necessários ao fornecimento do objeto, a citar especialmente:

2.18.1.1 - Instalar e configurar todos os produtos da solução (ferramentas) de auditoria para o ambiente Microsoft no serviço de Active Directory (AD) em fornecimento nos hardwares de destino:

2.18.1.2 - Instalar e configurar todos os produtos da solução (ferramentas) de auditoria para o ambiente Microsoft no serviço de Microsoft Exchange Server em fornecimento nos hardwares de destino;

2.18.1.3 - Instalar e configurar todos os produtos da solução (ferramentas) de auditoria para o ambiente Microsoft do serviço de Servidor de Arquivos Microsoft Windows Server em fornecimento nos hardwares de destino;

2.18.1.4 - Instalar e configurar todos os produtos da solução (ferramentas) de auditoria para o ambiente Microsoft do serviço de Servidor de Arquivos Microsoft Sharepoint Server em fornecimento nos hardwares de destino;

2.18.1.5 - Instalar e configurar todos os produtos da solução (ferramentas) de auditoria para o ambiente Unix/Linux Server em fornecimento nos hardwares de destino;

2.18.1.6 - Instalar e configurar o módulo de transferência automatizada de dados entre sistemas em fornecimento nos hardwares de destino;

Instalar e configurar o módulo de acesso de dados remoto em fornecimento nos hardwares de destino;

2.18.1.7 - Integrar todos os produtos (ferramentas) da solução de auditoria descritas no termo de referência;

2.18.1.8 - Demonstrar a utilização e a integração de todos os produtos (ferramentas) da solução de auditoria instalados no ambiente do ÓRGÃO e suas características funcionais (subitem 2.2), controle de acessos – controle de acesso (subitem 2.2.3), registro de eventos (subitem 2.4) e analise comportamental (subitem 2.2.5);

2.18.1.9 - Demonstrar a execução de todos os relatórios (item 2), identificação gráfica da analise comportamental conforme item 2, das notificações – alertas (subitem 2.2.6);

2.18.1.10 - Demonstrar a utilização e a integração de todos os produtos (ferramentas) da solução de auditoria para o ambiente Microsoft dos serviços do Microsoft Active Directory - AD (subitem 2.3), Microsoft Exchange Server (item 2.5) e Servidor de Arquivos Microsoft Windows Server (subitem 2.5), Microsoft SharePoint Server (subitem 2.6) e Unix/Linux File Server (item 2.7) no ambiente do ÓRGÃO;

2.19 - Execução de serviços profissionais de consultoria:

2.19.1 - Prestação de serviços de consultoria pós-implantação, na forma de um banco de horas, com em um total de 1.000 (um mil) horas de consultoria;

2.19.2 - Quando solicitadas, as horas demandadas pelo ÓRGÃO visam ao aperfeiçoamento do projeto implantado em termos da ferramenta de software instalada e dos serviços executados;

2.19.3 - Estes serviços deverão ser prestados sob demanda e localmente no ÓRGÃO (*on-site*), na modalidade 5x8 (cinco dias na semana, oito horas por dia – horário comercial);

2.19.4 - Para a prestação deste suporte técnico, a CONTRATADA somente poderá empregar profissionais capacitados e certificados nos produtos fornecidos;

2.19.5 - O ÓRGÃO oficializará a solicitação deste apoio por meio da emissão de uma "Ordem de Serviço – OS", sob demanda;

2.19.6 - A execução será sempre precedida da emissão pelo ÓRGÃO da competente "Ordem de Serviço – OS", contendo no mínimo: descrição do serviço, prazo para a execução do serviço, período para a execução do serviço, local da execução do serviço, especificações técnicas do serviço e produtos esperados;

2.19.7 - Uma "Ordem de Serviço – OS" somente estará autorizada após conferência e atesto do Gestor do Contrato;

2.19.8 - Toda "Ordem de Serviço - OS" deverá ser assinada pelo Gerente do Projeto, representante da CONTRATADA perante o ÓRGÃO, declarando a concordância da CONTRATADA em executar as atividades descritas na "Ordem de Serviço – OS", de acordo com as especificações estabelecidas pelo ÓRGÃO;

2.19.9 - Os serviços deverão estar sempre de acordo com as especificações constantes nas "Ordens de Serviços – OS";

2.19.10 - O controle da execução dos serviços se dará em 03 (três) momentos, a saber: no início da execução – quando a "Ordem de Serviço – OS" é emitida pelo ÓRGÃO, durante a execução – com o acompanhamento e supervisão de responsáveis do ÓRGÃO, e ao término da execução – com o fornecimento de "Relatórios de Atividade de Consultoria Especializada" pela CONTRATADA e atesto dos mesmos por responsáveis do ÓRGÃO;

2.19.11 - Todos os serviços prestados pela CONTRATADA deverão ser necessariamente documentados, registrados e entregues ao ÓRGÃO pela mesma;

2.19.12 - Os serviços de apoio pós-implantação deverão ser executados preferencialmente em horário comercial, de segunda a sexta-feira, excetuando-se naqueles casos que necessariamente haja intervenção em serviços de Produção;

2.19.13 - A partir da emissão da "Ordem de Serviço – OS", a CONTRATADA terá até 07 (sete) dias corridos para iniciar a sua execução, ressalvados os casos em que comprovadamente seja necessário um agendamento dos trabalhos;

2.20 - Serviços de Transferência de Conhecimentos

2.20.1 - A transferência de conhecimento será realizada em turmas composta de até 3 colaboradores e poderão ser CONTRATADA até 5 turmas na modalidade de ata de registro de preço;

2.20.2 - A transferência de conhecimento será realizada no ambiente do cliente;

2.20.3 - O instrutor do treinamento deverá ser certificado nos elementos da solução;

2.20.4 - A transferência de conhecimento deverá possuir, no mínimo, 24 horas de duração;

2.20.5 - A transferência de conhecimento deverá ser ministrada em língua portuguesa, enquanto o material de apoio poderá ser em língua inglesa.

2.21 - Serviços de Garantia

2.21.1 - Serviços de garantia pelo período de 36 (trinta e seis) meses, contados da data de emissão do Termo de Homologação, conforme teste a ser realizado para comprovação de todas as funcionalidades solicitadas, contemplando manutenção preventiva e corretiva, incluindo atualização de versões, assim como suporte técnico, tanto para os produtos (software) quanto para todos os serviços contemplados pelo objeto;

2.21.2 - A CONTRATADA deverá garantir que os serviços objeto deste Contrato atenderão ao padrão de qualidade exigido pela indústria de informática e pelo Órgão;

2.21.3 - O suporte deverá ser prestado na modalidade 24 x 7, através de e-mail e número telefônico 0800;

2.21.4 - Após a abertura do chamado a CONTRATADA deverá iniciar o atendimento em até 4 horas após a abertura do chamado.

4. CARACTERISTICAS DOS PRODUTOS

4.1 - Quantidade dos Produtos

4.1.1 - Registro de preços para aquisição de solução baseada em software totalmente compatível com ambiente Microsoft e servidor de arquivos UNIX, para implantação de auditoria, controle e gerência de permissionamento dos serviços de diretório (Microsoft Active Directory), servidor de arquivos (Microsoft File Server), servidor de colaboração SharePoint (Microsoft Sharepoint Server), Servidor de Arquivos UNIX/Linux e Correio Eletrônico (Microsoft Exchange Server) do CONTRATANTE, bem como execução de serviços de planejamento, consultoria, implementação e testes, além de transferência de conhecimentos, com garantia (manutenção e suporte técnico) pelo período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste Contrato.

4.2 - Processo Entrega dos Produtos

4.2.1 - Os produtos especificados no termo de referência deverão ser entregues no Conselho da Justiça Federal, endereço: Setor de Clubes Esportivos Sul, Trecho III, Polo 8, Lote 9, Brasília-DF, no prazo máximo de 30 dias (trinta) dias corridos após o recebimento do empenho.

4.3 - Recebimento e Aprovação dos Produtos

4.3.1 - O recebimento do software será provisório, para posterior teste de conformidade, verificação das especificações técnicas deste Contrato e da proposta comercial.

4.3.2 – O CONTRATANTE efetuará os testes de conformidade e verificação do software, em até 30 (trinta) dias após o recebimento provisório, para que seja configurado o recebimento definitivo sendo lavrado o Termo de Recebimento/Aceite Definitivo.

4.3.3 - Entende-se por cumprimento do prazo de entrega o recebimento do software e sua instalação, deixando-os operacionais para o aceite. O não cumprimento rigoroso do prazo de entrega, ou entrega parcial, ou entrega de configuração inferior a solicitada implicará em rescisão do Contrato a ser firmado pelo CONTRATANTE e a empresa CONTRATADA.

4.3.4 - Os softwares somente serão aceitos após minucioso teste de funcionamento pela equipe da CTEC. Por meio do teste será precedida a checagem das perfeitas condições físicas dos mesmos em nossos equipamentos, bem como do respectivo funcionamento e a conformidade com as especificações, considerando-se as características ofertadas.

4.3.5 - Os softwares serão novos e entregues acondicionados, adequadamente, de forma a permitir completa segurança durante o transporte, que será de inteira responsabilidade da CONTRATADA.

4.3.6 – O CONTRATANTE reserva-se no direito de proceder a conexão ou instalar nos equipamentos, produtos de hardware e software licenciados de outros fornecedores ou fabricantes, desde que tal iniciativa não implique danos físicos ao

equipamento e sem que isto constitua pretexto para a CONTRATADA se desobrigar da garantia de funcionamento.

4.4 - Penalidades pela Inconformidade na Entrega

4.4.1 - Caso haja alguma inconformidade na entrega, será solicitada à CONTRATADA alteração do Relatório de Entrega, com inserção das penalidades aplicadas. Em quaisquer casos de aplicação de glosas o responsável pela aplicação da penalidade deverá anexar os documentos e relatórios comprobatórios do não atendimento aos resultados esperados nos testes de aceitação;

4.4.2 - Em caso de impasse na aplicação de penalidades, essas serão dirimidas pelo Gestor do Contrato e o representante da CONTRATADA;

4.4.3 - Os Termos de Aceitação e entrega definitiva deverão ser aprovados pelos Fiscais Técnico e Requisitante e serão utilizados para a integração do processo de pagamento das notas fiscais.

5. GARANTIA

5.1 - A empresa CONTRATADA deverá fornecer garantia de funcionamento mínima de 36 (trinta e seis) meses "on-site", contados a partir da data do aceite dos equipamentos, efetuando manutenção corretiva, sem ônus para o CONTRATANTE.

5.1.1 - Entende-se por manutenção corretiva a série de procedimentos destinados a recolocar o software em perfeito estado de uso, compreendendo, inclusive, substituição, ajuste e reparos necessários, de acordo com os manuais e normas técnicas específicas, não incluindo o fornecimento de material de consumo.

6. OBRIGAÇÕES DAS PARTES

6.1 – Obrigações da CONTRATANTE :

6.1.1 - Proporcionar à CONTRATADA as condições necessárias à execução regular do Contrato;

6.1.2 - Fornecer à CONTRATADA todo tipo de informação essencial à realização dos serviços, atentando ao quesito de segurança e sigilo de dados;

6.1.3 - Promover a fiscalização do Contrato, sob aspectos quantitativos e qualitativos anotando em registro próprio as falhas detectadas e exigindo as medidas corretivas necessárias, bem como acompanhar o desenvolvimento do contrato, conferir a entrega dos materiais e atestar os documentos pertinentes, podendo ainda sustar, recusar, mandar fazer, refazer ou desfazer qualquer procedimento que não esteja de acordo com os termos contratuais;

6.1.4 - Comunicar prontamente à CONTRATADA qualquer anormalidade na execução do objeto, podendo recusar o recebimento dos materiais que estejam em desacordo com as especificações e condições estabelecidas no presente Contrato e nos TERMOS DE RECEBIMENTO/ACEITE DEFINITIVO;

6.1.5 - Pagar à CONTRATADA os valores relativos às soluções/softwares de Auditoria entregues, homologados e aceitos, conforme o Termo de Aceite, após o ateste da devida Nota Fiscal/Fatura;

6.1.6 - Aplicar as penalidades previstas para o caso de não cumprimento de cláusulas contratuais ou aceitar as justificativas apresentadas pela CONTRATADA;

6.1.7 - Verificar a regularidade da situação fiscal e dos recolhimentos sociais trabalhistas da CONTRATADA conforme determina a lei, antes de efetuar o pagamento devido;

6.2 – Obrigações da Contratada

6.2.1 - Promover a remoção, às suas expensas, do solução/software de Auditoria que estiverem em desacordo com as especificações deste Contrato, Edital e/ou aquele em que for constatado dano em decorrência de transporte ou acondicionamento indevido, providenciando a substituição dos mesmos no prazo máximo de 02 (dois) dias, contados da notificação que lhe for entregue oficialmente.

6.2.2 - Substituir em 48 horas após ser comunicado, o solução/software de Auditoria, que apresentarem avarias, ou outro problema qualquer que não permita sua utilização total.

6.2.3 - Assumir as responsabilidades pelos encargos fiscais e comerciais resultante da adjudicação da Licitação, bem como entregar os materiais cotados, mediante agendamento, de acordo com as especificações e demais condições estipuladas no Edital, no prazo máximo de 30 (trinta) dias para o CONTRATANTE, contados da data do recebimento do pedido de fornecimento, no horário das 08h às 12h e das 14 às 17h, de segunda a sexta feira, no endereço constante neste Contrato.

6.2.4 - A solução/software de Auditoria deverá ser entregue em sua condição original, contendo marca, modelo, referência, fabricante, procedência, prazo de garantia e assistência técnica, de acordo com a legislação em vigor, observadas as especificações técnicas contidas neste Contrato.

6.2.5 - Comunicar ao CONTRATANTE, no prazo máximo de 02 (dois) dias que anteceder o da entrega da solução/software de Auditoria, os motivos que impossibilitem o seu cumprimento.

6.2.6 - Informar o n. do Banco, Agência e Conta-corrente para efeito de pagamento.

6.2.7 - Cumprir integralmente as especificações e prazos definidos nos termos de garantia dos produtos, garantindo a qualidade dos produtos e seus periféricos.

6.2.8 - Apresentar, em conjunto com a Fatura/Nota Fiscal de fornecimento de bens, e os comprovantes previstos no artigo 36 da Instrução Normativa SLTI/MPOG n. 2 de 2008:

6.2.8.1 - Da regularidade fiscal, constatada através de consulta "on-line" ao Sistema de Cadastramento Unificado de Fornecedores – SICAF, ou na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei 8.666/93.

6.2.9 - Em caso do CONTRATANTE, constar antes de cada pagamento, irregularidades de situação da CONTRATADA junto ao SICAF, o pagamento não será suspenso, mas a CONTRATADA ficará obrigada a providenciar no prazo de 30 (trinta) dias corridos a sua regularização ou apresentar a sua defesa sob pena de Rescisão do Contrato.

6.2.10 - Manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse da CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste Contrato devendo orientar seus empregados nesse sentido.

6.2.11 - Assinar, quando da assinatura do contrato, por meio de seu representante, Termo de Compromisso em que se responsabilizará pela manutenção de sigilo e confidencialidade das informações a que possa ter acesso em decorrência da contratação.

6.2.12 - Garantir que seus funcionários em serviço na CONTRATANTE em virtude da presente contratação, deverão circular nas dependências da CONTRATANTE portando o crachá de identificação da empresa. O CONTRATANTE apenas fornecerá o crachá de acesso.

6.2.13 - Substituir qualquer um dos profissionais alocados desta contratação, cuja atuação, permanência ou comportamento seja reprovado pelo CONTRATANTE, prejudiciais e inconvenientes à execução dos serviços ou às normas da CONTRATADA.

6.2.14 - Prestar as informações e os esclarecimentos solicitados, no prazo máximo de 48 (quarenta e oito) horas, a contar da solicitação feita pelo Gestor do Contrato;

6.2.15 - Responder por quaisquer prejuízos que os profissionais de alocados para manutenção, causarem o CONTRATANTE ou a terceiros, decorrentes de ação ou omissão, procedendo imediatamente os reparos ou indenizações cabíveis e assumindo o ônus e a responsabilidade decorrente.

6.2.16 - Aceitar, nas mesmas condições contratadas, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor atualizado do Contrato.

6.2.17 - Levar imediatamente ao conhecimento do Gestor do Contrato qualquer fato extraordinário ou anormal que ocorrer na entrega dos Equipamentos de informática (desktop).

6.2.18 - Responsabilizar-se sobre todos os atos de seus profissionais, relacionados ao manuseio de arquivos de dados, sistemas computadorizados, softwares e equipamentos de propriedade do CONTRATANTE;

6.2.19 - Não transferir a outrem, no todo ou em parte, o objeto da presente contratação;

6.2.20 - Sob pena de rescisão contratual, não caucionar ou utilizar o contrato para qualquer operação financeira, sem prévia e expressa anuência do CONTRATANTE.

6.2.21 - Manter, durante toda a vigência do contrato, as condições de habilitação e de qualificação exigidas no processo licitatório.

6.2.22 - A CONTRATADA devera disponibilizar, a partir da assinatura do contrato, suporte técnico via telefone 0800 e/ou e-mail exclusivo para o CONTRATANTE, do

próprio fabricante ou da CONTRATADA (desde que atestada sua capacidade técnica pelo fabricante), de segunda a sexta-feira, no horário compreendido entre 08h00 (oito) e18h00 (dezoito) horas, sem ônus para o CONTRATANTE, visando agilizar os chamados e atendimentos técnicos. Esse atendimento deve abranger todo o hardware e softwares fornecidos com o equipamento.

6.2.23 - A CONTRATADA deverá indicar em sua Proposta Comercial as condições, sob as quais prestara a assistência técnica para realização das manutenções corretivas atendendo aos requisitos constantes deste Contrato.

6.2.24 - Quaisquer peças, componentes ou outros materiais que apresentarem defeitos de fabricação devem ser substituídos por originais, sem ônus para a CONTRATANTE. A CONTRATADA não poderá cobrar valores adicionais, tais como custos de deslocamento, alimentação, transporte, alojamento, trabalho em sábados, domingos e feriados ou em horário noturno, bem como qualquer outro valor adicional.

6.2.25 - A manutenção corretiva será realizada em qualquer dia da semana, no horário compreendido entre 8h e 18h, a pedido do CONTRATANTE.

6.2.26 - O início do atendimento deverá ocorrer no prazo de 24 (vinte e quatro) horas, dentro do horário estabelecido no item anterior, contado a partir da solicitação feita pelo CONTRATANTE.

6.2.27 - O término do reparo da solução/software de Auditoria deverá ocorrer no prazo de 48 (quarenta e oito) horas, contado a partir do início do atendimento:

6.2.28 - No caso da CONTRATADA não terminar o reparo do equipamento no prazo estabelecido no "6.2.27", deverá substituir imediatamente a solução/software de Auditoria por outro de sua propriedade, com características e capacidades iguais ou superiores ao substituído, em caráter provisório e temporário, pelo prazo máximo de 30 (trinta) dias corridos, contados a partir da data da substituição.

6.2.29 - Findo o prazo de 30 (trinta) dias corridos, a substituição da solução/software de Auditoria será definitiva a critério do CONTRATANTE.

6.2.30 - Quando da solicitação da manutenção corretiva, por meio de telefone, fac-símile ou e-mail, o CONTRATANTE fornecerá a CONTRATADA, para fins de abertura de chamado técnico, obrigatoriamente as seguintes informações:

6.2.30.1 - Código de fabricação ou número de série do equipamento se for o caso;

6.2.30.2 - Anormalidade observada;

6.2.30.3 - Nome do responsável pela solicitação;

6.2.30.4 - Número do telefone para contato;

6.2.30.5 - Número da Ordem de Serviço do CONTRATANTE

6.2.31 - Todas as solicitações feitas pelo CONTRATANTE serão registradas pela CONTRATADA para acompanhamento e controle da execução deste Contrato:

6.2.31.1 - A CONTRATADA apresentara um Relatório de Visita contendo data e hora do chamado e do início e termino do atendimento, identificação do componente defeituoso, as providencias adotadas e demais informações pertinentes;

6.2.31.2 - O Relatório deverá ser assinado pelo responsável pela solicitação de manutenção corretiva.

6.2.32 - Se durante a vigência do contrato, houver a necessidade de alteração de algum componente da solução/software de Auditoria, o mesmo deverá ser apresentado, pela CONTRATADA, a critério do CONTRATANTE, para avaliação técnica;

6.2.33 - Para execução dos serviços de manutenção a CONTRATADA somente poderá desconectar os componentes de hardware ou desinstalar qualquer software que estiverem instalados ou ligados à solução/software de Auditoria com previa autorização do CONTRATANTE;

6.2.34 - A CONTRATADA deverá garantir que os meios de armazenamento magnéticos e/ou óticos utilizados pelos seus técnicos, durante as manutenções, estão livres de qualquer código malicioso ("vírus, worms, trojans..."), voltado para a danificação ou degradação, tanto de dados, quanto de software ou hardware;

6.2.35 - Observar dentre as diretrizes de sustentabilidade, as: menor impacto sobre recursos naturais como flora, fauna, ar, solo e água; preferência para materiais, tecnologias e matérias-primas de origem local; maior eficiência na utilização de recursos naturais como água e energia; maior geração de empregos, preferencialmente com mão de obra local; maior vida útil e menor custo de manutenção do bem e da obra; uso de inovações que reduzam a pressão sobre recursos naturais; e origem ambientalmente regular dos recursos naturais utilizados nos bens, serviços e obras.

7. DA VIGÊNCIA DO CONTRATO

7.1 - O Contrato vigorará por 12 (doze) meses, a partir da data de 11/12/2015 a 10/12/2016 tendo sua eficácia após a publicação no Diário Oficial da União, podendo, a critério da Administração/CONTRATANTE, ser prorrogado por iguais períodos sucessivos, ao máximo de 60 (sessenta) meses, mediante elaboração de termos aditivos, consoante o disposto no art. 57, inciso II da Lei n. 8.666/93.

8. REAJUSTE

8.1 - Em hipótese alguma, será permitido o reajuste de preços do objeto deste Contrato.

9. DO VALOR DO CONTRATO E DA DOTAÇÃO FINANCEIRA

9.1 - O valor global estimado da contratação é de **R$ 551.609,00 (quinhentos e cinquenta e um mil e seiscentos e nove reais)**, correndo a despesa à conta dos recursos consignados ao CONTRATANTE, no presente exercício, sob a seguinte classificação:

Fonte: recursos oriundos de Contrato firmado entre o Conselho da Justiça Federal e a Caixa Econômica Federal.

N.º de Empenho: Não há

9.2 - No exercício subsequente a despesa correrá à conta de dotações orçamentárias que lhe forem destinadas, registrando-se por simples apostila o crédito e

empenho para sua cobertura, em conformidade com o parágrafo 8º do artigo 65 da Lei n. 8.666/1993.

10. DO PAGAMENTO

10.1 - O pagamento será feito mediante apresentação do Termo de Recebimento Definitivo, emitido pelo CONTRATANTE e Nota Fiscal/Fatura emitida pela CONTRATADA, consolidando os quantitativos entregues em conforme com os padrões exigidos neste Contrato, que deverá conter:

10.1.1 – Cópias de todos os Termos de Recebimento Provisório e Termos de Recebimento Definitivo das entregas realizadas e testadas no período;

10.1.2 – Uma entrega só será considerada realizada mediante emissão do Termo de Recebimento/Aceite Definitivo pelo CONTRATANTE.

10.2 – O Fiscal Requisitante terá 5(cinco) dias úteis, a contar do recebimento, para avaliar o Relatório de Entrega. Caso o mesmo esteja em conformidade com o Termo de Aceite Definitivo, o Fiscal Requisitante autorizará a emissão da Nota Fiscal. Do contrário, caberá a ele devolver o Termo de Recebimento/Aceite Definitivo para que a CONTRATADA faça os ajustes;

10.3 - O prazo para pagamento será de 5 (cinco) dias úteis, contados a partir da data da apresentação da Nota Fiscal/Fatura, acompanhada dos demais documentos comprobatórios do cumprimento das obrigações da CONTRATADA.

10.4 - Havendo erro na apresentação da Nota Fiscal/Fatura ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, o pagamento ficará pendente até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o CONTRATANTE.

10.5 - Nos termos do artigo 36, § 6°, da Instrução Normativa SLTI/MPOG n. 02, de 30/04/2008, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a CONTRATADA:

10.5.1 - Não produziu os resultados acordados;

10.5.2 - Deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

10.5.3 - Deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

10.6 - Antes do pagamento, o CONTRATANTE realizará consulta *on line* ao SICAF e, se necessário, aos sítios oficiais, para verificar a manutenção das condições de habilitação da CONTRATADA, devendo o resultado ser impresso, autenticado e juntado ao processo de pagamento.

10.7 - Quando não se identificar má-fé ou a incapacidade da empresa de corrigir a situação, poderá ser concedido o prazo de até 15 (quinze) dias para que a CONTRATADA regularize suas obrigações trabalhistas ou suas condições de habilitação, sob pena de rescisão contratual.

10.8 - Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, nos termos da Instrução Normativa n. 1.234, de 11 de janeiro de 2012, da Secretaria da Receita Federal do Brasil.

10.9 – Quanto ao Imposto sobre Serviços de Qualquer Natureza (ISSQN), será observado o disposto na Lei Complementar n. 116, de 2003, e legislação municipal aplicável.

10.10 – A CONTRATADA regularmente optante pelo Simples Nacional, instituído pelo artigo 12 da Lei Complementar n. 123, de 2006, não sofrerá a retenção quanto aos impostos e contribuições abrangidos pelo referido regime, em relação às suas receitas próprias, desde que, a cada pagamento, apresente a declaração de que trata o artigo 6° da Instrução Normativa RFB n. 1.234, de 11 de janeiro de 2012.

10.11 – O pagamento será efetuado por meio de Ordem Bancária de Crédito, mediante depósito em conta-corrente, na agência e estabelecimento bancário indicado pela CONTRATADA, ou por outro meio previsto na legislação vigente.

10.12 - Será considerada como data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

10.13 – O CONTRATANTE não se responsabilizará por qualquer despesa que venha a ser efetuada pela CONTRATADA, que porventura não tenha sido acordada no contrato.

10.14 – O CONTRATANTE fará nenhum pagamento à CONTRATADA, antes de quitada ou relevada a multa que porventura lhe tenha sido aplicada.

10.15 - Na contagem dos prazos estabelecidos neste Contrato para efeito de pagamento excluir-se-á o dia do início e incluir-se-á o dia do vencimento, só se iniciando e se vencendo os prazos em dia de expediente do CONTRATANTE e considerar-se-ão os dias consecutivos, exceto quando for explicitamente disposto em contrário.

10.16 - Na ocorrência de eventual atraso de pagamento, provocado exclusivamente pelo CONTRATANTE, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante a aplicação das seguintes fórmulas: (*IN 02/2008 M. Planejamento*)

I = (TX / 100) / 365
EM = I x N x VP, onde:
I = Índice de atualização financeira;
TX = Percentual da taxa de juros de mora anual;
EM = Encargos moratórios;
N = Nº de dias entre a data prevista para pagamento e a do efetivo pagamento; e
VP = Valor da parcela em atraso.

11. SANÇÕES ADMINISTRATIVAS

11.1 - Pela inexecução ou execução parcial das condições assumidas no Contrato o CONTRATANTE aplicará à CONTRATADA, garantindo o contraditório e à prévia defesa, nos termos do art. 87, da Lei n. 8.666/93, com suas ulteriores alterações, as seguintes sanções:

I - Advertência, por escrito;

II – Multa de 2% (dois por cento) do valor do contrato, por dia de atraso injustificado na prestação dos serviços e/ou no descumprimento das demais obrigações contratuais assumidas, até o limite de 15 (quinze) dias, contados a partir da detecção da falta ou atraso verificado;

III - multa de 5% (cinco por cento), do valor total do Contrato, a partir do 16º (décimo sexto) dia de atraso injustificado na prestação dos serviços e/ ou no descumprimento das demais obrigações contratuais assumidas, até o 30º (trigésimo) dia, configurando-se, após o referido prazo, a inexecução total deste Contrato;

IV - multa de 10% (dez por cento) sobre o valor total atualizado do Contrato, após o prazo acima mencionado e/ ou no caso de reincidência do descumprimento de quaisquer das cláusulas contratuais, aplicada cumulativamente com as demais sanções, ensejando, inclusive, a rescisão do Contrato;

V - suspensão temporária do direito de participar em licitação e impedimento de contratar com o CONTRATANTE, por prazo de até 02 (dois) anos, conforme a autoridade ministerial competente fixar, em função da natureza e gravidade da falta cometida.

VI - declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação, perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir a Administração pelos prejuízos resultantes, e depois de decorrido o prazo da sanção aplicada com base na alínea anterior.

11.2 - Decorrido o prazo de 10 (dez) dias corridos para o recolhimento de multa, ao débito será acrescido 1% (um por cento) de mora por mês/fração, inclusive referente ao mês da quitação/consolidação do débito, limitado o pagamento com atraso em até 60 (sessenta) dias após a data da notificação e, após este prazo, o débito poderá ser cobrado judicialmente.

11.3- Se a multa aplicada for superior ao valor dos pagamentos eventualmente devidos, responderá a CONTRATADA pela sua diferença, podendo ser esta cobrada judicialmente.

11.4 - As multas não têm caráter indenizatório e seu pagamento não eximirá a CONTRATADA de ser acionada judicialmente pela responsabilidade civil derivada de perdas e danos junto o CONTRATANTE, decorrentes das infrações cometidas.

12. DO ACOMPANHAMENTO E FISCALIZAÇÃO

12.1 - Durante a vigência do contrato com prestação de garantia de funcionamento os serviços de suporte técnico serão acompanhados e fiscalizados por servidor da Secretaria de Tecnologia do CONTRATANTE, designado com essa finalidade, permitida o acompanhamento por colaborador da empresa prestadora de serviço terceirizada atuante no órgão para assisti-los e subsidiá-los de informações pertinentes a essa atribuição;

12.2 - Os representantes do CONTRATANTE anotarão em registro próprio todas as ocorrências relacionadas com o fornecimento dos itens adquiridos e a execução dos serviços mencionados, determinando o que for necessário à regularização das faltas ou defeitos observados;

12.3 - A CONTRATADA deverá indicar responsável técnico para representá-la durante o fornecimento e garantia das licenças e a execução dos serviços ora tratados, desde que aceito pelo CONTRATANTE;

13. DA PUBLICAÇÃO

13.1 – O CONTRATANTE publicará, no Diário Oficial da União, o extrato deste contrato, até o quinto dia útil do mês seguinte ao de sua assinatura, para ocorrer no prazo de até 20 (vinte) dias daquela data, nos termos do parágrafo único do art. 61, da Lei n. 8.666/93, com suas posteriores alterações.

14. DOS CASOS OMISSOS

14.1 - Os casos omissos relacionados a este Contrato regular-se-ão pelos preceitos de direito público aplicando-se-lhes, supletivamente, os princípios da teoria geral dos contratos e as disposições de direito privado, na forma dos arts. 54 e 55, inciso XII, da Lei n. 8.666, de 1993.

15. DO FORO

15.1 - As partes elegem o foro da Justiça Federal, Seção Judiciária do Distrito Federal, para dirimir quaisquer dúvidas relativas ao cumprimento deste instrumento, desde que não possam ser dirimidas pela mediação administrativa, renunciando a qualquer outro, por mais privilegiado que seja.

15.2 - E por estarem assim justas e acertadas celebram o presente contrato em 02 (duas) vias de igual teor e forma, para um só efeito, o qual, depois de lido e achado conforme, perante duas testemunhas a todo o ato presentes, vai pelas partes assinado.

Brasília-DF, 04 de dezembro de 2015.

EVA MARIA FERREIRA BARROS
Diretora-Geral do Conselho da Justiça Federal

HIRAN RICARDO FRANCO DA SILVA
Vice-Presidente da empresa
Vert Soluções em Informática Ltda

Testemunhas:

a) _____
Nome: Alexandre Lameiro
CPF n. 706.075.351-49

b) _____
Nome: Celeni R. L. da Silva
CPF n. 480.382.101-15

Vert Soluções em TIC Jurídico

PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

ANEXO I AO CONTRATO N. 034/2015 – CJF

TERMO DE REFERÊNCIA

1. OBJETO

1.1 Registro de Preço para aquisição de solução baseada em software totalmente compatível com ambiente Microsoft e servidor de arquivos UNIX, para implantação de auditoria, controle e gerência de permissionamento dos serviços de diretório (Microsoft Active Directory), servidor de arquivos (Microsoft File Server), servidor de colaboração SharePoint (Microsoft Sharepoint Server), Servidor de Arquivos UNIX/Linux e Correio Eletrônico (Microsoft Exchange Server) da EMBRATUR, bem como execução de serviços de planejamento, consultoria, implementação e testes, além de transferência de conhecimentos, com garantia (manutenção e suporte técnico) pelo período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste Termo de Referência.

2. FUNDAMENTAÇÃO LEGAL

2.1. A contratação de pessoa jurídica, para fornecimento de solução baseada em software de auditoria, controle e gerência de permissionamento dos serviços de diretório, objeto do presente Termo de Referência, encontra amparo legal na seguinte legislação:
a. Lei nº. 8.666, de 21 de junho de 1993, com suas alterações subsequentes;
b. Lei nº. 10.520, de 7 de julho de 2002;
c. Decreto nº. 3.555, de 08 de agosto de 2000, alterados pelos Decretos nos 3.693, de 20 de dezembro de 2000 e 3 784, de 06 de abril de 2001;
d. Decreto nº. 5.450 de 31 de maio de 2005;
e. Decreto nº. 2.271, de 07 de julho de 1997;
f. Instrução Normativa nº. 02, de 30 de abril de 2008;
g. Instrução Normativa nº. 04, de 12 de novembro de 2010;
h. Instrução Normativa 01/2010 – SLTI/MP;
i. Portaria nº 2, de 16 de março 2010, da SLTI/MP.

3. JUSTIFICATIVA

3.1 O Instituto Brasileiro de Turismo – EMBRATUR é responsável pela promoção, marketing e apoio à comercialização dos destinos, serviços e produtos turísticos brasileiros no mercado internacional.
3.2 Para o cumprimento de tal missão é necessário dispor de recursos que viabilizem a consecução das estratégias, objetivos e metas estabelecidas. E dentre estes recursos tornaram-se imprescindíveis os relacionados à Tecnologia da Informação.
3.3 Assim, objetivando a sustentação dos produtos e serviços de TI demandados pela organização se faz necessário a contratação de ferramenta capaz de auditar os recursos instalados no parque computacional da EMBRATUR.

4. RESULTADOS ESPERADOS

4.1 Os resultados a serem alcançados com a aquisição da ferramenta, deve dotar o parque tecnológico da EMBRATUR atendendo aos padrões de qualidade, em condições de capacidade e desempenho que proporcionem à EMBRATUR aplicar a Tecnologia da Informação - TI ao negócio de maneira eficiente e segura em cumprimento de sua missão institucional.
Os resultados esperados são:
4.1.1 Assegurar a qualidade e disponibilidade dos equipamentos no parque tecnológico da EMBRATUR;
4.1.2 Assegurar o controle da base de dados e monitorar o uso e a aplicação das ferramentas já disponíveis aos usuários.
4.1.3 Prover a infraestrutura de dispositivos e ferramentas de auditagem no banco de dados e demais equipamentos em uso.
4.1.4 Ampliar com o uso da ferramenta a qualidade e a confiabilidade das informações contidas nos bancos de dados da EMBRATUR.

4.2 Produtos esperados pela contratação

4.2.1 Solução baseada em softwares para auditoria, controle e gerência de permissionamento dos serviços de diretório (Microsoft Active Directory), servidor de arquivos (Microsoft File Server), servidor de colaboração SharePoint (Microsoft Sharepoint Server), Servidor de Arquivos UNIX/Linux e Correio Eletrônico (Microsoft Exchange Server);

4.2.2 Serviços de implementação e testes;
4.2.3 Serviços de consultoria;
4.2.4 Serviços de transferência de conhecimentos;
4.2.5 Garantia (manutenção e suporte técnico);

4.3 Resultados esperados com a contratação

4.3.1 Visão completa da estrutura do diretório da Microsoft, 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;
4.3.2 Auditoria eficiente do Active Directory, Exchange, servidor de arquivos e SharePoint Server, que por meio dos logs de auditoria você tem visibilidade de todos os eventos ocorridos;
4.3.3 Auditoria eficiente do sistema de arquivos de sistemas Linux e Unix, através da visibilidade dos eventos ocorridos;
4.3.4 Possibilidade de migração automatizada de dados entre equipamentos com a necessária manutenção ou alteração de metadados de auditoria e segurança;
4.3.5 Possibilidade de acesso aos arquivos através da Internet com segurança e auditoria do acesso aos arquivos;
4.3.6 Gestão do permissionamento e dos logs de todas as plataformas monitoradas em uma única console;
4.3.7 Relatórios visando facilitar o controle sobre o que acontece em todos os ambientes;
4.3.8 Alertas de modificação, quando alguma ação for disparada;
4.3.9 Consultas e pesquisas de eventos.

5. ESPECIFICAÇÃO TECNICA DA SOLUÇÃO

5.1 Objetiva-se com a contratação efetuar a implantação de uma solução de auditoria, controle e gerência de permissionamento dos serviços de diretório (Microsoft Active Directory, LDAP e NIS), servidor de arquivos (Microsoft File Server), servidor de colaboração SharePoint (Microsoft Sharepoint Server), Servidor de Arquivos UNIX/Linux e Correio Eletrônico (Microsoft Exchange Server), os quais são responsáveis pela comunicação e armazenamento dos dados não estruturados do ÓRGÃO, contemplando:
5.1.1 Licenciamento completo de até 500 usuários internos
5.1.2 Execução de serviços profissionais para implementação e testes, para até 500 usuários, possibilitando a aquisição dos serviços em lotes de até 500 usuários internos, de acordo com o item 5.1.
5.1.3 Instalação e configuração da solução (softwares) no ambiente da CONTRATANTE;
5.1.4 Integração e compartilhamento de recursos e auditoria, controle, gerenciamento e permissionamento da solução com o ambiente de produção existente;
5.1.5 Execução de serviços profissionais de até 1.000 horas de consultoria para customização e ajustes dos itens adquirido no item 5.1, a serem executados dentro do prazo vigente do contrato;
5.1.6 Transferência de conhecimentos composta por turmas de 3 alunos, possibilitando a aquisição de até 5 turmas na modalidade de ata de registro de preços;
5.1.7 Serviço de manutenção e suporte pelo período de 36 (trinta e seis) meses;

5.2 Descrição detalhada da solução

5.2.1 Características funcionais:
5.2.1.1 A solução ofertada deverá reter as informações de log e histórico em banco de dados (MS SQL ou Oracle), seja ele na máquina local ou em SQL Farm já existente dentro do ÓRGÃO por um período que será determinado na fase de escopo do projeto (mínimo de 12 meses);
5.2.1.2 As licenças do ambiente operacional para instalação do produto, incluindo o Sistema Operacional e o banco de dados para a solução serão fornecidos pela CONTRATANTE;
5.2.1.3 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;
5.2.1.4 A solução deverá contemplar na mesma console a possibilidade de englobar as funcionalidades através de agentes adicionais para no mínimo as plataformas, Microsoft Active Directory, LDAP, NIS, Microsoft Exchange Server, Microsoft Sharepoint Server e Windows Server e UNIX Servers;
5.2.1.5 Caso a solução utilize um agente nos servidores a serem monitorados, sua instalação não deve requerer a reinicialização dos mesmos;
5.2.1.6 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;
5.2.1.7 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;
5.2.1.8 A solução deve fornecer método para assinalar ou associar um usuário como "Proprietário" de uma pasta ou grupo;
5.2.1.9 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;
5.2.1.10 Deve permitir o gerenciamento das funcionalidades através de console própria ou por navegador WEB;
5.2.1.11 Fornecer interface única de usuário para exibir as permissões, os detalhes da auditoria, as estatísticas de acesso a dados e alertas;
5.2.1.12 A solução deve suportar a utilização de servidores Virtualizados (VMWare) para todos os seus componentes;
5.2.1.13 A solução deve contemplar o licenciamento dos bancos de dados e sistemas operacionais para a instalação e monitoração da solução;

5.3 Controle de acessos (permissionamento)

5.3.1 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;
5.3.2 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, subgrupos e seus respectivos membros;
5.3.3 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;
5.3.4 A solução deve permitir a visibilidade bidirecional de quais pastas podem ser acessadas por quais usuários e na direção contrária, indicando todas as pastas onde o usuário tem acesso e qual tipo de acesso (leitura, escrita, modificação), sem afetar o ambiente em operação;
5.3.5 A ferramenta deverá prover filtros para visualizar todos os objetos de dados de forma gráfica incluindo pastas protegidas e únicas;
5.3.6 A solução deverá fornecer a visão das permissões efetivas, ou seja, agregando permissões de Share e NTFS;
5.3.7 A ferramenta não deve restringir a quantidade das listas de acesso (ACLs) coletadas e/ou armazenadas;
5.3.8 A visualização de grupos deve compreender todos os grupos filhos (subgrupos) sem restrição de número de hierarquias;
5.3.9 A solução deve possibilitar a configuração de uma credencial diferente para cada volume a ser monitorado;
5.3.10 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;
5.3.11 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;
5.3.12 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;
5.3.13 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;

5.4 Registro de eventos (log)

5.4.1 A solução deve coletar o log de forma normatizada dos repositórios de dados em plataforma Serviço de Diretórios, Servidores de Arquivos Windows e UNIX/LINUX, Sharepoint e Microsoft Exchange;
5.4.2 A solução ofertada deve manter o log das operações de abrir, criar, apagar, modificar, copiar, renomear e acesso negado;
5.4.3 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;
5.4.4 Deverá permitir filtragem gráfica, ordenação e agrupamento dos logs;
5.4.5 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;
5.4.6 Fornecer resumo gráfico das atividades auditadas, incluindo:

5.2.3.7 Visualização dos usuários mais e menos ativos;
5.2.3.8 Visualização dos diretórios mais e menos ativos;
5.2.3.9 Visualização dos diretórios onde um usuário ou um grupo de usuários estejam acessando;
5.2.3.10 Visualização dos usuários que estejam acessando um diretório;
5.2.3.11 A ferramenta deve normatizar eventos relacionados e apresentar como um único evento para o mesmo objeto;
5.2.3.12 A solução deve permitir auditoria direta de quem tem acesso aos dados na tela da console, sem necessidade de gerar relatório demonstrativo.

5.5 Relatórios

5.5.1 A solução ofertada deve gerar relatórios nos formatos TXT, CSV, HTML, XLS e PDF;
5.5.2 A ferramenta deve permitir o agendamento para envio de relatórios pelo correio eletrônico;
5.5.3 Os relatórios agendados devem poder ser entregues tanto via e-mail quanto em uma determinada pasta do servidor sem a necessidade de customização adicional;
5.5.4 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;
5.5.5 A ferramenta deve possibilitar a definição da prioridade de cada relatório agendado;
5.5.6 A ferramenta deve fornecer relatórios customizáveis sob demanda e agendados;
5.5.7 A ferramenta deve fornecer relatório dos acessos aos arquivos;
5.5.8 A ferramenta deve armazenar todas as modificações feitas nas permissões dentro e fora da interface gráfica;
5.5.9 Fornecer relatórios sobre onde a permissões concedidas a grupos globais (Everyone, Domain Users, Users) estão sendo utilizadas;
5.5.10 Armazenar todas as modificações em grupos feitas dentro e fora da interface gráfica;
5.5.11 Fornecer relatórios de grupos de segurança vazios ou não utilizados;
5.5.12 Fornecer relatórios de SIDs não resolvidos e usuários com permissão direta em pastas;
5.5.13 Fornecer relatórios de dados e usuários inativos;
5.5.14 Fornecer relatórios sobre administradores acessando dados de negócio;
5.5.15 Fornecer relatórios de usuários desabilitados que ainda fazem parte de grupos de segurança;
5.5.16 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;
5.5.17 Possibilitar o direito de revisão de gestão de dados através de relatórios indicativos do uso dos dados;
5.5.18 Suprir com rotinas automatizadas, relatórios programados e outras facilidades sobre os benefícios esperados, destes relatórios;
5.5.19 A solução deve ser capaz de fornecer relatórios para auditoria e conformidade (compliance);

5.6 Analise Comportamental

5.6.1 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;
5.6.2 A solução deve identificar, de forma automática, usuários com acesso a pastas e\ou arquivos indevidos sugerindo a revogação de acesso;
5.6.3 A solução deverá fornecer em modo gráfico recomendações sobre permissionamento excessivo, baseado na análise de atividade de acesso;
5.6.4 Fornecer identificação gráfica de atividades de acesso anormais;
5.6.5 Estas recomendações deverão também ser fornecidas em forma de relatório;

5.7 Sistema de notificações (alertas)

5.7.1 A ferramenta deve realizar análises e gerar alertas de comportamentos suspeitos como leitura ou gravações em excessos que diferem do comportamento normal do usuário;
5.7.2 A notificação deverá ser feita também via e-mail;
5.7.3 A ferramenta deve emitir um alerta quando um usuário desviar do seu comportamento padrão;
5.7.4 Fornecer relatórios sobre atividades de acesso anormais;

5.8 Módulo Permissionamento de Serviços Active Directory (AD)

5.8.1 A solução deve efetuar as funcionalidades de Permissionamento, Log, Relatórios, Alertas dos serviços de diretórios de usuários como Microsoft Active Directory, LDAP, NIS e usuários locais dos servidores, e deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios de dados;
5.8.2 A solução deve possuir visibilidade da hierarquia dos Serviço de Diretórios dos Usuários através de interface gráfica e em formato de relatório;

Ver. Soluções e TIC Jurídico PRM

5.8.3 Solução deve possuir visibilidade da hierarquia dos Serviço de Diretórios dos Usuários através de interface gráfica e em formato de relatório;
5.8.4 A solução deve ter trilha de auditoria classificável e pesquisável de todas as atividades do Active Directory, LDAP, NIS e usuários locais dos servidores em uma única interface gráfica e também em formato de relatório;
5.8.5 Solução deverá ser capaz rastrear quem fez alterações no Active Directory, LDAP, NIS e usuários locais dos servidores, qual foi a alteração feita e quando, nesta mesma interface gráfica e em formato de relatório;
5.8.6 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;
5.8.7 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, permitindo a visibilidade anterior à realização das alterações no permissionamento de qual o impacto real no ambiente de produção;
5.8.8 A solução ofertada deverá suportar o gerenciamento do Microsoft Active Directory ao ponto de permitir os administradores da solução no mínimo as seguintes funcionalidades:
5.8.8.1 Criação de novos usuários;
5.8.8.2 Criação de novos grupos;
5.8.8.3 Alteração de parâmetros de usuários já existentes;
5.8.8.4 Deleção de usuários;
5.8.8.5 Deleção de computadores;
5.8.8.6 Reset de senhas;
5.8.8.7 Desbloqueio de usuários;
5.8.8.8 Desabilitação de usuários;
5.8.9 A solução deverá ser compatível, no mínimo, com as versões do Microsoft AD 2003, 2008 e 2012;

5.9 Módulo Microsoft Exchanger Server

5.9.1 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;
5.9.2 A solução ofertada deverá monitorar as caixas postais dos usuários, e as pastas compartilhadas deste servidor;
5.9.3 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;
5.9.3.1 Caso a solução necessite a ativação do Journaling do Exchange deverá ser fornecido o hardware necessário para o armazenamento deste journaling por 12 (doze) meses;
5.9.4 As funcionalidades de análise comportamental deverão ser realizada dentro das pastas compartilhadas e caixas de correios dos servidores Microsoft Exchange monitorados;
5.9.5 A ferramenta ofertada deverá coletar os eventos dos servidores de e-mail monitorados contemplando no mínimo os seguintes itens:
5.9.5.1 Mensagem aberta;
5.9.5.2 Mensagem enviada;
5.9.5.3 Mensagem enviada "como" (on behalf of);
5.9.5.4 Mensagem enviada "em nome de;
5.9.5.5 Mensagem editada;
5.9.5.6 Mensagem apagada;
5.9.5.7 Mensagem movida / copiada;
5.9.5.8 Mensagem marcada como lida / não lida;
5.9.5.9 Definição de sinalizadores;
5.9.5.10 Pasta aberta;
5.9.5.11 Pasta criada / apagada;
5.9.5.12 Permissões adicionadas / removidas / alteradas;
5.9.5.13 Pasta movida / copiada;
5.9.5.14 Anexo aberto;
5.9.5.15 Anexo apagado / adicionado;
5.9.5.16 Delegação de caixa de correio adicionada / removida;
5.9.5.17 Logon;
5.9.5.18 Permissões de caixa de correio adicionadas / removidas;
5.9.6 A solução deverá auditar, registrar eventos (log) e aplicar as análises comportamentais das caixas postais e pastas compartilhadas do Microsoft Exchange Server para eventos gerados a partir de dispositivos moveis

acessos externos (via internet) por meio de acesso WEB através dos seguintes protocolos de comunicação contemplando no mínimo os seguintes itens:
5.9.6.1 POP3 – Post Office Protocol v3;
5.9.6.2 IMAP – Internet Message Access Protocol;
5.9.6.3 MAPI - Messaging Application Programming Interface;
5.9.6.4 OWA – Outlook Web Access;
5.9.6.5 EWS – Exchange Web Services;
5.9.6.6 ActiveSync - para smartphones e outros dispositivos similares.
5.9.7 A solução deverá registrar eventos (logs) contendo informações do IP de origem do dispositivo móvel ou computador de onde foi acessada a caixa postal;
5.9.8 A solução deve ser compatível com o Microsoft Exchange Server no mínimo nas versões 2007 e 2010;

5.10 Módulo Microsoft Windows Server:

5.10.1 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;
5.10.2 A solução deve ter sua compatibilidade certificada em Windows Server 2003, 2008 e 2012;
5.10.3 Deverá suportar às tecnologias DAS, SAN, Windows-Powered NAS e suporte à tecnologia de cluster da Microsoft;
5.10.4 Integrar com as plataformas de storage existentes VNX da EMC e NetAPP sem a necessidade de instalação de softwares ou agentes;

5.11 Módulo Microsoft Sharepoint Server:

5.11.1 A solução deve efetuar as funcionalidades de permissionamento, Log, Relatórios, Análise Comportamental e Alerta descrita nos itens acima em plataformas de servidores de arquivos Microsoft Office Sharepoint Server:
5.11.2 A solução deve ter sua compatibilidade certificada em Microsoft Office Sharepoint Server x64 e x86 para as plataformas 2007, 2010 e 2013;

5.12 Módulo Microsoft UNIX Server:

5.12.1 A solução deve efetuar as funcionalidades de Permissionamento, Log, Relatórios, Análise Comportamental e Alertas descritos nos itens acima em plataformas de servidores de arquivos LINUX.
5.12.2 A solução deve ter sua compatibilidade certificada em no mínimo as seguintes versões:
5.12.2.1 Red Hat 4 Kernel 2.6.9:
a) smp - 32 bit;
b) Hugemem - 32 bit;
c) smp - 64 bit;
d) LargeSmp - 64 bit.
5.12.2.2 Red Hat 5 Kernel 2.6.18:
a) smp - 32 bit
b) xen–smp - 32 bit;
c) pae–smp - 32 bit;
d) smp - 64 bit
5.12.2.3 Red Hat 6 Kernel 2.6.32:
a) smp - 32 bit;
b) smp - 64 bit
5.12.2.4 SUSE SLES 10 Kernel 2.6.16:
a) xenpae-smp - 32 bit;
b) smp - 64 bit
5.12.2.5 Ubuntu 8.04 LTS Kernel 2.6.24:
a) smp – 32 and 64 bit;
5.12.2.6 Ubuntu 10.04 LTS Kernel 2.6.32-38:
a) smp - 64 bit;
b) pae-smp - 32 bit

5.13 Módulo Portal de Permissionamento:

5.13.1 A solução deverá permitir que os usuários donos das pastas permitam acesso aos seus dados não-estruturados e semiestruturados a outros usuários, bem como a revogação destes acessos, sem necessidade de envolvimento do administrador do sistema;
5.13.2 Ter interface web para solicitação de permissionamento/participação em grupo de segurança;
5.13.3 Ser capaz de personalizar um fluxo de aprovação para cada demanda do usuário;
5.13.4 Enviar e-mail de notificação ao aprovador/dono da informação quando uma nova

solicitação for aberta a ele:
5.13.4.1 Possibilitar a escolha de uma data de expiração/validade do permissionamento aprovado;
5.13.4.2 Revogar automaticamente as permissões escolhidas na sua data de expiração sem que se faça necessária a intervenção de um usuário;
5.13.4.3 Criar revisões de permissionamento direcionadas diretamente ao dono de cada pasta/grupo;
5.13.4.4 Sinalizar nas revisões de permissionamento, quais usuários poderiam ter suas permissões removidas sem que haja impacto ao negócio;
5.13.4.5 Disponibilizar para o responsável por cada conjunto de dados, acesso aos logs de auditoria, estatísticas e permissões;
5.13.4.6 Permitir a criação de regras de segurança para que usuários ou grupos de usuários nunca tenham acesso a determinado conjunto de dados;
5.13.4.7 Forçar as regras de segurança para que caso uma permissão seja concedida diretamente, o software as remova sem a intervenção de um usuário;
5.13.5 A solução deverá prover a habilidade de identificar os proprietários dos dados e enviar aos mesmos relatórios sobre permissionamento e acesso.

5.14 Módulo Migração de Dados Automatizados entre plataformas:

5.14.1 A solução deve permitir a migração de dados entre plataformas no mínimo:
5.14.1.1 CIFS para Sharepoint:
a) Deve permitir a personalização e simulação nas alterações de permissões antes da migração. (Ex.: a critério do administrador a permissão "Leitura" no CIFS se tornará "Contribuir" no Sharepoint, a permissão "Modificar" se tornará "Gerenciar Hierarquia", etc
5.14.1.2 Sharepoint para CIFS
5.14.2 A solução deve permitir a migração de dados entre domínios:
5.14.2.1 A solução deve permitir migrar mantendo as permissões, metadados e ACL's;
5.14.2.2 A solução deve automaticamente, na migração entre domínios, criar novos grupos no active directory, mantendo assim as mesmas permissões de usuários que estavam no antigo repositório.
5.14.3 A solução deve permitir configurar e programar o horário e com qual frequências as migrações irão ocorrer.
5.14.4 A solução deve permitir migrar dados em horário de produção sem que haja interrupção ao usuário e perdas de dados;
5.14.5 A solução deve permitir a migração dos dados com base nas recomendações sugeridas pela ferramenta de auditoria;
5.14.6 A solução deve permitir migrar alterando as permissões de acordo com as recomendações;
5.14.7 A solução deve permitir em interface gráfica simular o impacto da migração baseadas nas regras definidas;
5.14.8 A solução deve permitir ao administrador, refinar e editar as permissões ACL's antes da migração;
5.14.9 A solução deve ter a capacidade de simular os efeitos de permissão sobre os utilizadores pós-migração;
5.14.10 A solução deve permitir deixar as permissões como estão ou torna-las melhor com base nas recomendações feitas pela solução de auditoria;
5.14.11 A solução deve permitir migrações incrementais, baseadas somente nos dados novos ou alterados do primeiro repositório;
5.14.12 A solução deve permitir migrar mantendo as mesmas estruturas de hierarquia de pastas no novo repositório;
5.14.12.1 A solução deve ter a opção de migrar todo o conteúdo das pastas ou somente a estrutura de pastas;
5.14.13 A solução deve possuir algoritmo para identificar e solucionar colisões em nomes de arquivos e pastas;
5.14.14 A solução deve através de metadados e regras de classificação possibilitar a identificação de arquivos e pastas e migrar entre plataformas, domínios distintos, mantendo as permissões, metadados e ACL's;
5.14.15 A solução deve permitir a identificação de dados não acessados por determinado período de tempo e migrar entre plataformas, domínios distintos, mantendo as permissões, metadados e ACL's;
5.14.16 A solução deve em conjunto com a a ferramenta de classificação possibilitar a migração de dados sensíveis entre plataformas, domínios distintos, mantendo as permissões, metadados e ACL's;
5.14.17 A solução deve através de metadados possibilitar a identificação de arquivos por extensão, tamanho, nome, e migrar entre plataformas, domínios distintos, mantendo as permissões, metadados e ACL's;
5.14.18 A solução deve através da ferramenta de auditoria possibilitar a identificação de mais usados e migrar entre plataformas, domínios distintos, mantendo as permissões, metadados e ACL's;

5.14.19 A solução deve permitir criar regras de migração automática, continua e única, possibilitando assim que qualquer arquivo ou documento novo incluído no repositório de dados, seja automaticamente migrado entre plataformas, domínios distintos, mantendo as permissões, metadados e ACL's;
5.14.20 A solução deve permitir criar regras de migração automática, baseadas em regras de negócio, migrado entre plataformas, domínios distintos, mantendo as permissões, metadados e ACL's.

5.15 Módulo Acesso de dados remotos:

5.15.1 A solução deverá suportar o acesso simultâneos para a quantidade de usuário adquiridas, de acordo com o item 5.1.2.
5.15.2 A solução ofertada deve permitir que os sistemas de arquivos, CIFS e NFS, atualmente implementados no ÓRGÃO seja compartilhados de maneira segura para os usuários externos e internos;
5.15.3 A solução deverá realizar a função de proxy e streamline de acesso seguro (HTTPS) para a o servidor de arquivos já implementada com base nos protocolos NFS e CIFS;
5.15.4 A comunicação entre a solução ofertada e repositório de usuário, para autenticação dos mesmos, se dará através do protocolo LDAP;
5.15.5 A autenticação deve utilizar base de usuários dos diretórios de serviços corporativos, sendo compatíveis com bases LDAP v.3 e Microsoft Active Directory, sem a necessidade de criação de base interna para esta finalidade;
5.15.6 A autenticação dos usuários deverá ocorrer através do protocolo HTTPS sem a necessidade de certificados digitais ou VPN;
5.15.7 A sincronia de dados entre a solução e o cliente deverá ser realizada através do protocolo HTTPS;
5.15.8 O cliente deve notificar os usuários para cada alteração feita nos arquivos;
5.15.9 Solução deverá implementar a sincronia automática entre arquivos e pastas armazenados nos repositórios CIFS e NFS do ÓRGÃO e os clientes da solução, como computadores, laptops, smartphones e tablets dos funcionários internos e externos de maneira segura. No mínimo para os seguintes clientes;
5.15.10 Windows (Vista, 7 ou superior);
5.15.11 Apple iOS (iPhone e iPad);
5.15.12 Android;
5.15.13 A solução deve possibilitar a adição de novos arquivos e arquivos editados, através de smartphones e tablets;
5.15.14 A solução deve possibilitar o acesso aos compartilhamentos e arquivos através do navegador WEB;
5.15.15 Os arquivos devem ser disponibilizados sem a utilização de serviços externos e utilização de cache a própria solução, devendo armazenar os arquivos estritamente nos repositórios internos e nos clientes autorizados para a solução;
5.15.16 A sincronia entre os dispositivos deverá ocorrer sem que haja a necessidade de alocação de novos espaços, com a criação de novos arquivos ou pastas, nos repositórios atualmente em utilização;
5.15.17 As permissões para acesso aos arquivos e pastas devem obedecer as mesmas regras definidas para a base de usuários existente, expressas no compartilhamento CIFS e NFS;
5.15.18 Deve ser possível o fornecimento de links web para compartilhamento de arquivos, pastas e um espaço para upload de arquivos para colaboradores externos ao ÓRGÃO, desde que autorizado pelo administrador da rede
5.15.19 O acesso aos arquivos e diretórios realizados por colaboradores externos deve possuir dois modos de compartilhamentos, conforme descrito abaixo;
5.15.20 Público: Permite o acesso aos dados por qualquer um que possua o link;
5.15.21 Privado: O acesso será permitido somente ao usuário destinatário, através do uso de uma senha de identificação (pin) que será alterada em cada acesso realizado pelo colaborador externo;
5.15.22 Para cada uma das pastas adicionadas ao serviço de compartilhamento e sincronia deve ser possível a definição do tipo de compartilhamento, com no mínimo as seguintes opções;
5.15.23 Compartilhamento Externo;
5.15.24 Compartilhamento Interno;
5.15.25 Compartilhamento Externo e Interno;
5.15.26 Deve permitir a definição de data de expiração para o compartilhamento das pastas e arquivos;
5.15.27 A solução deverá fornecer uma pasta para upload para uso de colaboradores externos;
5.15.28 A solução não deve restringir o tamanho dos arquivos compartilhados;
5.15.29 A Pasta de upload deve permitir o controle de validade (tempo) e tamanho de arquivos;
5.15.30 Solução deve emitir um alerta para o administrador informando que arquivos e pastas internas foram compartilhados com colaboradores externos;

5.15.31 A Solução deverá controlar o acesso aos dados mantendo registro das operações de abrir, criar, apagar, modificar, copiar renomear e de acesso negado;
5.15.32 Deverá implementar a coleta de log de forma normatizada dos repositórios de dados Windows e Linux;

5.11 Módulo de Classificação de Dados sensiveis e integração com DLP

5.11.1 A solução deve ser capaz de de identificar qual dado ou arquivo contém informações sensíveis ou confidenciais.
A solução deve identificar dados sensíveis nas plataformas Windows e NAS.
5.11.3 A solução deve exibir na mesma interface gráfica informações sobre os permissionamentos, ACL's , quantidade de informações sensíveis e qual tipo de informação sensivel classificada, afim de facilitar a identificação de potenciais repositórios e pastas super expostos.
5.11.4 A solução deve gerar em forma de relatórios dados sobre a classificação das informações.
5.11.5 A solução deve ter a capacidade de Incluir filtros sobre a classificação dos dados nas pesquisas dos Logs.
5.11.6 A solução deve ter a capacidade de Incluir filtros sobre a classificação dos dados nos relatórios de acesso.
5.11.7 Para cada arquivo marcado como sensível, a solução deve possibilitar a visão, diretamente da ferramenta, das expressões regulares ou strings que fizeram com que esse arquivo fosse considerado como sensível
5.11.8 A solução deve fornecer visibilidade de conteúdo crítico de negócios através da classificação da informação.
5.11.9 A ferramenta deve fornecer visibilidade dos locais que possuem dados sensíveis.
5.11.10 A solução deve gerar recomendações acionáveis para redução de acesso aos dados classificados como sensíveis.
5.11.11 A solução deve integrar a funcionalidade de classificação de dados sensíveis com soluções de terceiros para estender a habilidade de ambos.
5.11.12 A solução deve possibilitar a instalação da funcionalidade de classificação de dados sensíveis em um único servidor, sem a necessidade de servidores adicionais.
5.11.13 A solução deve fornecer a funcionalidade de busca de arquivos através de palavras-chave, frases e/ou expressões regulares.
5.11.14 A ferramenta deve 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
5.11.15 A solução deve classificar dados utilizando mecanismo de busca proprio capaz de pesquisar conteudos sensíveis atraves de "strings", expressões regulares ou regras pré-definidas;
5.11.16 A solução deverá realizar uma busca dentro de arquivos word, excel, pdf, txt. Dos conteúdos identificados como sensíveis e delimitados nas "strings" Deve ser possível priorizar a ordem pelas quais os arquivos sensíveis serão buscados, como por exemplo, filtrar primeiramente os mais acessados, os maiores, entre outros

5.12 Demais Componentes

5.12.1 Todos os componentes passivos adicionais que se fizerem necessários para efetivar as interligações dos ativos do objeto da contratação;
5.12.2 Visando preservar harmonia entre todos os elementos da solução, a total interoperabilidade de componentes e a facilidade de uso e operação, a solução fornecida deverá ser de um único fabricante em que seus módulos e ou programas sejam totalmente integrados e disponibilizados em uma única console de gerência;
5.12.3 O modulo (esquema) de segurança da solução (software) não deverá implicar em aquisição de componentes (hardware e software) adicionais;
5.12.4 Deverá ser compatível e permitir a utilização da tecnologia "hyperthreading" sem custos adicionais;
5.12.5 A solução deverá possibilitar integração, de forma direta ou indireta, de suas informações com sistemas de DLP (Data Lost Prevention);

5.13 Módulo Serviços profissionais para implementação e testes

5.13.1 Execução de todos os serviços profissionais para Implementação e Testes necessários ao fornecimento do objeto, a citar especialmente:
5.13.2 Instalar e configurar todos os produtos da solução (ferramentas) de auditoria para o ambiente Microsoft no serviço de Active Directory (AD) em fornecimento nos hardwares de destino:
5.13.3 Instalar e configurar todos os produtos da solução (ferramentas) de auditoria para o ambiente Microsoft no serviço de Microsoft Exchange Server em fornecimento nos hardwares de destino;
5.13.4 Instalar e configurar todos os produtos da solução (ferramentas) de auditoria para o ambiente Microsoft do serviço de Servidor de Arquivos Microsoft Windows Server em fornecimento nos hardwares de destino;
5.13.5 Instalar e configurar todos os produtos da solução (ferramentas) de auditoria para o ambiente Microsoft do serviço de Servidor de Arquivos Microsoft Sharepoint Server em fornecimento nos hardwares de destino;

5.13.6 Instalar e configurar todos os produtos da solução (ferramentas) de auditoria para o ambiente Unix/Linux Server em fornecimento nos hardwares de destino;
5.13.7 Instalar e configurar o modulo de transferência automatizada de dados entre sistemas em fornecimento nos hardwares de destino;
5.13.8 Instalar e configurar o modulo de acesso de dados remoto em fornecimento nos hardwares de destino;
5.13.9 Integrar todos os produtos (ferramentas) da solução de auditoria descritas neste termo de referência;
5.13.10 Demostrar a utilização e a integração de todos os produtos (ferramentas) da solução de auditoria instalados no ambiente do ÓRGÃO e suas características funcionais (subitem 5.2), controle de acessos – controle de acesso (subitem 5.2.3), registro de eventos (subitem 5.4) e analise comportamental (subitem 5.2.5);
5.13.11 Demostrar a execução de todos os relatórios (item 5), identificação gráfica da analise comportamental conforme item 5, das notificações – alertas (isubitem 5.2.6);
5.13.12 Demostrar a utilização e a integração de todos os produtos (ferramentas) da solução de auditoria para o ambiente Microsoft dos serviços do Microsoft Active Directory - AD (subitem 5.3),
Microsoft Exchange Server (item 5.5) e Servidor de Arquivos Microsoft Windows Server (subitem 5.5), Microsoft SharePoint Server (subitem 5.6) e Unix/Linux File Server (item 5.7) no ambiente do ÓRGÃO;
5.14 Execução de serviços profissionais de consultoria:
5.14.1 Prestação de serviços de consultoria pós-implantação, na forma de um banco de horas, com em um total de 1.000 (um mil) horas de consultoria;
5.14.2 Quando solicitadas, as horas demandadas pelo ÓRGÃO visam ao aperfeiçoamento do projeto implantado em termos da ferramenta de software instalada e dos serviços executados;
5.14.3 Estes serviços deverão ser prestados sob demanda e localmente no ÓRGÃO (on-site), na modalidade 5 x 8 (cinco dias na semana, oito horas por dia – horário comercial);
5.14.4 Para a prestação deste suporte técnico, a CONTRATADA somente poderá empregar profissionais capacitados e certificados nos produtos fornecidos;
5.14.5 O ÓRGÃO oficializará a solicitação deste apoio por meio da emissão de uma "Ordem de Serviço – OS", sob demanda;
5.14.6 A execução será sempre precedida da emissão pelo ÓRGÃO da competente "Ordem de Serviço – OS", contendo no mínimo: descrição do serviço, prazo para a execução do serviço, período para a execução do serviço, local da execução do serviço, especificações técnicas do serviço e produtos esperados;
5.14.7 Uma "Ordem de Serviço – OS" somente estará autorizada após conferência e atesto do Gestor do Contrato;
5.14.8 Toda "Ordem de Serviço – OS" deverá ser assinada pelo Gerente do Projeto, representante da CONTRATADA perante o ÓRGÃO, declarando a concordância da CONTRATADA em executar as atividades descritas na "Ordem de Serviço – OS", de acordo com as especificações estabelecidas pelo ÓRGÃO;
5.14.9 Os serviços deverão estar sempre de acordo com as especificações constantes nas
"Ordens de Serviços – OS";
5.14.10 O controle da execução dos serviços se dará em 03 (três) momentos, a saber: no início da execução – quando a "Ordem de Serviço – OS" é emitida pelo ÓRGÃO, durante a execução – com o acompanhamento e supervisão de responsáveis do ÓRGÃO, e ao término da execução com o fornecimento de "Relatórios de Atividade de Consultoria Especializada" pela CONTRATADA e atesto dos mesmos por responsáveis do ÓRGÃO;
5.14.11 Todos os serviços prestados pela CONTRATADA deverão ser necessariamente documentados, registrados e entregues ao ÓRGÃO pela mesma;
5.14.12 Os serviços de apoio pós-implantação deverão ser executados preferencialmente em horário comercial, de segunda a sexta-feira, excetuando-se naqueles casos que necessariamente haja intervenção em serviços de Produção;
5.14.13 A partir da emissão da "Ordem de Serviço – OS", a CONTRATADA terá até 07 (sete) dias corridos para iniciar a sua execução, ressalvados os casos em que comprovadamente seja necessário um agendamento dos trabalhos;
5.15 Serviços de Transferência de Conhecimentos
5.15.1 A transferência de conhecimento será realizada em turmas composta de até 3 colaboradores e poderão ser contratadas até 5 turmas na modalidade de ata de registro de preço;
5.15.2 A transferência de conhecimento será realizada no ambiente do cliente;
5.15.3 O instrutor do treinamento deverá ser certificado nos elementos da solução;
5.15.4 A transferência de conhecimento deverá possuir, no mínimo, 24 horas de duração;
5.15.5 A transferência de conhecimento deverá ser ministrada em língua portuguesa, enquanto o material de apoio poderá ser em língua inglesa.

5.16 Serviços de Garantia

5.16.1 Serviços de garantia pelo período de 36 (trinta e seis) meses, contados da data de emissão do Termo de Homologação, conforme teste a ser realizado para comprovação de todas as funcionalidades solicitadas, contemplando manutenção preventiva e corretiva, incluindo atualização de versões, assim como suporte técnico, tanto para os produtos (software) quanto para todos os serviços contemplados pelo objeto;

5.16.2 A CONTRATADA deverá garantir que os serviços objeto deste Termo de Referência atenderão ao padrão de qualidade exigido pela indústria de informática e pelo Órgão;

5.16.3 O suporte deverá ser prestado na modalidade 24 x 7, através de e-mail e número telefônico 0800;

5.16.4 Após a abertura do chamado a CONTRATADA deverá iniciar o atendimento em até 4 horas após a abertura do chamado.

6. CRITÉRIOS DE SUSTENTABILIDADE

6.1 Por se tratar de aquisição de bens, com a finalidade de nortear os critérios de sustentabilidade, deverão ser observados as normas contidas no Capítulo III, DOS BENS E SERVIÇOS, com ênfase nos arts. 5º e 6º da Instrução Normativa nº 01, de 19 de janeiro de 2010, bem como, o Decreto nº 7.746, de 05 de junho de 2012 que estabelece os critérios, práticas e diretrizes para a promoção do desenvolvimento nacional sustentável;

6.2 São diretrizes de sustentabilidade, a serem observadas pela CONTRATADA, entre outras:
menor impacto sobre recursos naturais como flora, fauna, ar, solo e água; preferência para materiais, tecnologias e matérias-primas de origem local; maior eficiência na utilização de recursos naturais como água e energia; maior geração de empregos, preferencialmente com mão de obra local; maior vida útil e menor custo de manutenção do bem e da obra; uso de inovações que reduzam a pressão sobre recursos naturais; e origem ambientalmente regular dos recursos naturais utilizados nos bens, serviços e obras;

6.3 A CONTRATADA deverá apresentar para efeito de assinatura do contrato declaração expressa que atende aos critérios de sustentabilidade ambiental quanto aos processos de extração ou fabricação, utilização e descarte dos produtos e matérias primas em cumprimento à instrução normativa nº 01/2010.

7. CARACTERÍSTICAS DOS PRODUTOS

7.1 QUANTIDADE DOS PRODUTOS

7.1.1 Registro de preços para aquisição de solução baseada em software totalmente compatível com ambiente Microsoft e servidor de arquivos UNIX, para implantação de auditoria, controle e gerência de permissionamento dos serviços de diretório (Microsoft Active Directory), servidor de arquivos (Microsoft File Server), servidor de colaboração SharePoint (Microsoft Sharepoint Server), Servidor de Arquivos UNIX/Linux e Correio Eletrônico (Microsoft Exchange Server) da EMBRATUR, bem como execução de serviços de planejamento, consultoria, implementação e testes, além de transferência de conhecimentos, com garantia (manutenção e suporte técnico) pelo período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste Termo de Referência.

7.2 PROCESSO DE ENTREGA DOS PRODUTOS

7.2.1 Os produtos especificados neste termo de referência deverão ser entregues em cada repartição pública, conforme a localidade de cada orgão participante, no prazo máximo de 30 (trinta) dias corridos após o recebimento do empenho.

7.3 RECEBIMENTO E APROVAÇÃO DOS PRODUTOS

7.3.1 O recebimento do software será provisório, para posterior teste de conformidade, verificação das especificações técnicas deste Termo de Referência e da proposta comercial.

7.3.2 A EMBRATUR efetuará os testes de conformidade e verificação do software, em até 30 (trinta) dias após o recebimento provisório, para que seja configurado o recebimento definitivo sendo lavrado o Termo de Recebimento/Aceite Definitivo.

7.3.3 Entende-se por cumprimento do prazo de entrega o recebimento do software e sua instalação, deixando-os operacionais para o aceite. O não cumprimento rigoroso do prazo de entrega, ou entrega parcial, ou entrega de configuração inferior a solicitada implicará em rescisão do contrato a ser firmado pela EMBRATUR e a empresa CONTRATADA.

7.3.4 O software somente serão aceitos após minucioso teste de funcionamento pela equipe da CTEC. Por meio do teste será precedida a checagem das perfeitas condições físicas dos mesmos em nossos equipamentos, bem como do respectivo funcionamento e a conformidade com as especificações, considerando-se as características ofertadas.

7.3.5 O software serão novos e entregues acondicionados, adequadamente, de forma a permitir completa segurança durante o transporte, que será de inteira responsabilidade da CONTRATADA.
7.3.6 A EMBRATUR, reserva-se no direito de proceder a conexão ou instalar nos equipamentos, produtos de hardware e software licenciados de outros fornecedores ou fabricantes, desde que tal iniciativa não implique danos físicos ao equipamento e sem que isto constitua pretexto para o licitante vencedor se desobrigar da garantia de funcionamento.

8. PRAZO DE GARANTIA

8.1 A empresa CONTRATADA deverá fornecer garantia de funcionamento mínima de 36 (trinta e seis) meses "on-site", contados a partir da data do aceite dos equipamentos, efetuando manutenção corretiva, sem ônus para a EMBRATUR.
8.1.1 Entende-se por manutenção corretiva a série de procedimentos destinados a recolocar o software em perfeito estado de uso, compreendendo, inclusive, substituição, ajuste e reparos necessários, de acordo com os manuais e normas técnicas específicas, não incluindo o fornecimento de material de consumo.

9. PENALIDADES PELA INCONFORMIDADE NA ENTREGA

9.1 Caso haja alguma inconformidade na entrega, será solicitada à CONTRATADA alteração do Relatório de Entrega, com inserção das penalidades aplicadas. Em quaisquer casos de aplicação de glosas o responsável pela aplicação da penalidade deverá anexar os documentos e relatórios comprobatórios do não atendimento aos resultados esperados nos testes de aceitação;
9.2 Em caso de impasse na aplicação de penalidades, essas serão dirimidas pelo Gestor do Contrato e o representante da CONTRATADA;
9.3 Os Termos de Aceitação e entrega definitiva deverão ser aprovados pelos Fiscais Técnico e Requisitante e serão utilizados para a integração do processo de pagamento das notas fiscais.

10. ESTIMATIVA DE PREÇO E ORÇAMENTO

10.1 Para a estimativa de preço do software de auditoria junto as empresas vencedoras dos recentes processos licitatórios de órgãos da Administração Pública Federal e ou disponível no mercado.

10.2 **Assim, com base no valor médio calculado o valor estimado dos quantitativos para contratação para a EMBRATUR é de R$ 1.755.515,88 (Hum milhão, setecentos e cinquenta e cinco mil, quinhentos e quinze reais e oitenta e oito centavos);**
10.3 O recurso orçamentário para atender a despesa está previsto no Orçamento Geral da EMBRATUR, Recursos do Tesouro – Exercício Corrente - Ação nº 23.122.2128.2000.0001.

10.4 PROCESSO LICITATÓRIO/REGISTRO DE PREÇOS

10.4.1 O Sistema de Registro de Preços (SRP) é o conjunto de procedimentos para registro formal de preços relativos à prestação de serviços e aquisição de bens, para contratações futuras;
10.4.3 Portanto, Optou-se por fazer o registro de preços em conformidade com o disposto no Decreto nº 7892/2013, no seu Art. 3º, item IV;
11.4.3 A demanda visa dar segurança, Padronização de Procedimentos, Centralização de Informações, Indicadores e Rastreabilidade. Esta aquisição foi aprovada na 6ª reunião de Comitê Gestor de Tecnologia da Informação, porém devido ao contingenciamento de orçamento deste Instituto será providenciado o processo licitatório e a contratação se dará na liberação de dotação orçamentária.

11. MODELO DE GESTÃO DE CONTRATO

11.1 PAPÉIS E RESPONSABILIDADES

11.1.1 O **FISCAL REQUISITANTE**, disponibilizado pela CONTRATANTE, será responsável por:
11.1.1.1 Supervisionar o recebimento dos produtos e emitir Termo de recebimento provisório e encaminhá-lo ao Fiscal Técnico para avaliação técnica e teste de entrega conforme descrito item 5 e 6.
11.1.1.2 Indicar a aplicação de glosas, referente aos itens em desacordo com os padrões de qualidade exigidos;
11.1.1.3 Anexar documentos comprobatórios do não atendimento às exigências, para aplicação de aplicação de glosas.
11.1.2 O **FISCAL TÉCNICO**, disponibilizado pela CONTRATANTE, será responsável por:
11.1.2.1 Receber o software, avaliar a compatibilidade contratual, registrar, autorizar e encaminhar à CONTRATADA;

11.1.2.2 Acompanhar e fiscalizar a execução das instalação da solução/software e anotar em registro próprio todas as ocorrências relacionadas efetiva entrada em operação dos mesmos, comunicando ao gestor do contrato ocorrências de quaisquer fatos que exijam medidas corretivas;
11.1.2.3 Determinar as datas e os horários para realização das manutenções, em acordo com a área demandante, prevendo o mínimo de impacto nas atividades dos usuários;
11.1.3 O **FISCAL ADMINISTRATIVO**, disponibilizado pela CONTRATANTE, será responsável por:
11.1.3.1 Permitir o acesso dos representantes e dos recursos técnicos da CONTRATADA ao local de prestação dos serviços de manutenção, desde que devidamente identificados e respeitadas as normas que disciplinam a segurança do patrimônio, das pessoas e das informações da EMBRATUR;
11.1.3.2 Proporcionar todas as condições necessárias para que a CONTRATADA possa cumprir o objeto desta contratação;
11.1.3.3 Fiscalizar, com apoio da área técnica, o cumprimento das exigências legais por parte da CONTRATADA, tais como verificação das comprovações de regularidade jurídica, trabalhistas e fiscal.
11.1.4 A CONTRATADA indicará como **RESPONSÁVEL**, profissional com atribuição para realizar a interlocução com o Gestor do Contrato e Fiscais da EMBRATUR. É dele a responsabilidade de consolidar os Termos de Recebimento e;
11.1.4.1 Receber as Ordens de Serviço de manutenção e encaminhar aos técnicos responsáveis pela execução, subsidiando com o que for necessário;
11.1.4.2 Informar à EMBRATUR sobre problemas de quaisquer natureza que possam impedir o bom andamento das entregas e dos serviços de manutenção;

11.2 SANÇÕES ADMINISTRATIVAS E PENALIDADES

11.2.1 Pela inexecução total ou parcial do instrumento de contrato, a EMBRATUR poderá, garantida a prévia defesa, aplicar à CONTRATADA as seguintes sanções:
Art. 87. Pela inexecução total ou parcial do contrato a Administração poderá, garantida a prévia defesa, aplicar ao contratado as seguintes sanções:
a) I - Advertência, por escrito;
b) II - Multas;
c) III - Suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior à 02 (dois) anos;
d) IV - Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.
11.2.2 O valor correspondente a qualquer multa aplicada à CONTRATADA poderá ser descontado: de acordo com o estabelecido, ou ainda, a critério da EMBRATUR respeitado o princípio do contraditório e ampla defesa, da garantia prevista no contrato, ou dos pagamentos, ou recolhidas à conta Única do Tesouro Nacional em favor da EMBRATUR, no prazo de 10 (dez) dias corridos contados a partir do recebimento da notificação, ou ainda, se for o caso, poderão ser cobradas judicialmente, nos termos dos parágrafos 2º e 3º, do art. 86 da Lei 8.666/93.
11.2.3 Decorrido o prazo de 10 (dez) dias corridos para o recolhimento de multa, o débito será acrescido 1% (um por cento) de mora por mês/fração, inclusive referente ao mês da quitação/consolidação do débito, limitado o pagamento com atraso em até 60 (sessenta) dias após a data da notificação e, após este prazo, o débito poderá ser cobrado judicialmente.
11.2.4 No caso de a CONTRATADA ser credora de valor suficiente, a EMBRATUR poderá proceder ao desconto da multa devida na proporção do crédito.
11.2.5 Se a multa aplicada for superior ao valor dos pagamentos eventualmente devidos, responderá a CONTRATADA pela sua diferença, podendo ser esta cobrada judicialmente.
11.2.6 As multas não têm caráter indenizatório e seu pagamento não eximirá a CONTRATADA de ser acionada judicialmente pela responsabilidade civil derivada de perdas e danos junto a EMBRATUR, decorrentes das infrações cometidas.

11.3 PAGAMENTO

11.3.1 O faturamento será mediante apresentação do Termo de Recebimento definitivo emitido pela contratante e Nota Fiscal emitida pela CONTRATADA, consolidando os quantitativos entregues em conformidade com os padrões exigidos neste Termo de Referência, que deverá conter:
a. Cópias de todos os TERMOS DE RECEBIMENTO PROVISÓRIO E TERMOS DE RECEBIMENTO DEFINITIVO das entregas realizadas e testadas no período;

11.3.2 Uma entrega só será considerada realizada mediante emissão do TERMO DE RECEBIMENTO/ACEITE DEFINITIVO pela CONTRATANTE;
11.3.3 O Fiscal Requisitante terá 5 (cinco) dias úteis, a contar do recebimento, para avaliar o Relatório de Entrega. Caso o mesmo esteja em conformidade com o Termo de Aceite Definitivo, o Fiscal Requisitante autorizará a emissão da Nota Fiscal. Do contrário, caberá a ele devolver o TERMO DE RECEBIMENTO/ACEITE DEFINITIVO para que a CONTRATADA faça os ajustes;
11.3.4 A nota Fiscal emitida pela CONTRATADA deverá ser atestada pelo Fiscal Requisitante e pelo Gestor do Contrato e encaminhada para a área administrativa efetuar o pagamento, acompanhada do TERMO DE RECEBIMENTO/ACEITE DEFINITIVO, e da documentação comprobatória multas ou glosas por ventura existente, todos aprovados e assinados pelo responsável Requisitante.

12. VIGÊNCIA E PRAZO PARA ASSINATURA DO CONTRATO

12.1 O prazo para assinatura do contrato será de 10 (dez) dias úteis, contados a partir da data de convocação pela CONTRATANTE, podendo ser prorrogado uma vez, por igual período, quando solicitado pela parte e desde que ocorra motivo justificado e aceito pelo órgão;
12.2 Em hipótese alguma, será permitido o reajuste de preços no contrato objeto deste termo de Referência (solução/software de Auditoria).

13. OBRIGAÇÕES DA CONTRATANTE

13.1 Proporcionar à CONTRATADA as condições necessárias à execução regular do Contrato;
13.2 Fornecer à CONTRATADA todo tipo de informação essencial à realização dos serviços, atentando ao quesito de segurança e sigilo de dados;
13.3 Promover a fiscalização do contrato, sob aspectos quantitativos e qualitativos anotando em registro próprio as falhas detectadas e exigindo as medidas corretivas necessárias, bem como acompanhar o desenvolvimento do contrato, conferir a entrega dos materiais e atestar os documentos pertinentes, podendo ainda sustar, recusar, mandar fazer, refazer ou desfazer qualquer procedimento que não esteja de acordo com os termos contratuais;
13.4 Comunicar prontamente à CONTRATADA qualquer anormalidade na execução do objeto, podendo recusar o recebimento dos materiais que estejam em desacordo com as especificações e condições estabelecidas no presente Termo de Referência e nos TERMOS DE RECEBIMENTO/ACEITE DEFINITIVO;
13.5 Pagar à CONTRATADA os valores relativos aos solução/software de Auditoria entregues, homologados e aceitos, conforme o Termo de Aceite, após o ateste da devida Nota Fiscal/Fatura;
13.6 Aplicar as penalidades previstas para o caso de não cumprimento de cláusulas contratuais ou aceitar as justificativas apresentadas pela CONTRATADA;
13.7 Verificar a regularidade da situação fiscal e dos recolhimentos sociais trabalhistas da CONTRATADA conforme determina a lei, antes de efetuar o pagamento devido;

14. OBRIGAÇÕES DA CONTRATADA

14.1 Promover a remoção, às suas expensas, do solução/software de Auditoria que estiverem em desacordo com as especificações deste Termo de Referência, Edital e/ou aquele em que for constatado dano em decorrência de transporte ou acondicionamento indevido, providenciando a substituição dos mesmos no prazo máximo de 02 (dois) dias, contados da notificação que lhe for entregue oficialmente.
14.2 Substituir em 48 horas após ser comunicado, o solução/software de Auditoria, que apresentarem avarias, ou outro problema qualquer que não permita sua utilização total
14.3 Assumir as responsabilidades pelos encargos fiscais e comerciais resultante da adjudicação da Licitação, bem como entregar os materiais cotados, mediante agendamento, de acordo com as especificações e demais condições estipuladas no Edital, no prazo máximo de 30 (trinta) dias para a EMBRATUR, contados da data do recebimento do pedido de fornecimento, no horário das 08h às 12h e das 14 às 17h, de segunda a sexta feira, nos endereços constante neste Termo de Referência.
14.4 A solução/software de Auditoria deverão ser entregues em sua condição original, contendo marca, modelo, referência, fabricante, procedência, prazo de garantia e assistência técnica, de acordo com a legislação em vigor, observadas as especificações técnicas contidas neste Termo de referência.
14.5 Comunicar a EMBRATUR, no prazo máximo de 02 (dois) dias que anteceder o da entrega da solução/software de Auditoria, os motivos que impossibilitem o seu cumprimento;
14.6 Informar o nº do Banco, Agência e Conta corrente para efeito de pagamento
14.7 Cumprir integralmente as especificações e prazos definidos nos termos de garantia dos produtos, garantindo a qualidade dos produtos e seus periféricos;
14.8 Apresentar, em conjunto com a Fatura/Nota Fiscal de fornecimento de bens, e os comprovantes previstos no artigo 36 da Instrução Normativa SLTI/MPOG nº 2 de 2008:

I - da regularidade fiscal, constatada através de consulta "on-line" ao Sistema de Cadastramento Unificado de Fornecedores – SICAF, ou na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art 29 da Lei 8.666/93;

14.9 Em caso do CONTRATANTE, constar antes de cada pagamento, irregularidades de situação da CONTRATADA junto ao SICAF, o pagamento não será suspenso, mas a CONTRATADA ficará obrigada a providenciar no prazo de 30 dias corridos a sua regularização ou apresentar a sua defesa sob pena de Rescisão do contrato.

14.10 Manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse da CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste Contrato devendo orientar seus empregados nesse sentido;

14.11 Assinar, quando da assinatura do contrato, por meio de seu representante, Termo de Compromisso em que se responsabilizará pela manutenção de sigilo e confidencialidade das informações a que possa ter acesso em decorrência da contratação;

14.12 Garantir que seus funcionários em serviço na EMBRATUR em virtude da presente contratação, deverão circular nas dependências da CONTRATANTE portando o crachá de identificação da empresa. A EMBRATUR apenas fornecerá o crachá de acesso;

14.13 Substituir qualquer um dos profissionais alocados desta contratação, cuja atuação, permanência ou comportamento seja reprovado pela CONTRATANTE, prejudiciais e inconvenientes à execução dos serviços ou às normas da EMBRATUR;

14.14 Prestar as informações e os esclarecimentos solicitados, no prazo máximo de 48 (quarenta e oito) horas, a contar da solicitação feita pelo Gestor do Contrato;

14.15 Responder por quaisquer prejuízos que os profissionais de alocados para manutenção, causarem a EMBRATUR ou a terceiros, decorrentes de ação ou omissão, procedendo imediatamente os reparos ou indenizações cabíveis e assumindo o ônus e a responsabilidade decorrente;

14.16 Aceitar, nas mesmas condições CONTRATADAs, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor atualizado do contrato;

14.17 Levar imediatamente ao conhecimento do Gestor do Contrato qualquer fato extraordinário ou anormal que ocorrer na entrega dos Equipamentos de informática (desktop);

14.18 Responsabilizar-se sobre todos os atos de seus profissionais, relacionados ao manuseio de arquivos de dados, sistemas computadorizados, softwares e equipamentos de propriedade da EMBRATUR;

14.19 Não transferir a outrem, no todo ou em parte, o objeto da presente contratação;

14.20 Sob pena de rescisão contratual, não caucionar ou utilizar o contrato para qualquer operação financeira, sem prévia e expressa anuência da EMBRATUR;

14.21 Manter, durante toda a vigência do contrato, as condições de habilitação e de qualificação exigidas no processo licitatório;

14.22 A licitante vencedora devera disponibilizar, a partir da assinatura do contrato, suporte técnico via telefone 0800 e/ou e-mail exclusivo para a EMBRATUR, do próprio fabricante ou da CONTRATADA (desde que atestada sua capacidade técnica pelo fabricante), de segunda a sexta-feira, no horário compreendido entre 08h00 (oito) e18h00 (dezoito) horas, sem ônus para a EMBRATUR, visando agilizar os chamados e atendimentos técnicos. Esse atendimento deve abranger todo o hardware e softwares fornecidos com o equipamento;

14.23 A licitante vencedora deverá indicar em sua Proposta Comercial as condições, sob as quais prestara a assistência técnica para realização das manutenções corretivas atendendo aos requisitos constantes deste Termo de Referência;

14.24 Quaisquer peças, componentes ou outros materiais que apresentarem defeitos de fabricação devem ser substituídos por originais, sem ônus para a CONTRATANTE. A CONTRATADA não poderá cobrar valores adicionais, tais como custos de deslocamento, alimentação, transporte, alojamento, trabalho em sábados, domingos e feriados ou em horário noturno, bem como qualquer outro valor adicional.

14.25 A manutenção corretiva será realizada em qualquer dia da semana, no horário compreendido entre 08:00 (oito) e 18:00 (dezoito) horas, a pedido da EMBRATUR.

14.26 O início do atendimento deverá ocorrer no prazo de 24 (vinte e quatro) horas, dentro do horário estabelecido no item anterior, contado a partir da solicitação feita pela EMBRATUR

14.27 O término do reparo da solução/software de Auditoria deverá ocorrer no prazo de 48 (quarenta e oito) horas, contado a partir do início do atendimento:

14.28 No caso da licitante vencedora não terminar o reparo do equipamento no prazo estabelecido no "14.3", deverá substituir imediatamente a solução/software de Auditoria por outro de sua propriedade, com características e capacidades iguais ou superiores ao substituído, em caráter provisório e temporário, pelo prazo máximo de 30 (trinta) dias corridos, contados a partir da data da substituição;

Verti Soluções em TIC Jurídico PFM

14.29 Findo o prazo de 30 (trinta) dias corridos, a substituição da solução/software de Auditoria será definitiva a critério da EMBRATUR.
14.30 Quando da solicitação da manutenção corretiva, por meio de telefone, fac-símile ou e-mail, a EMBRATUR fornecerá a licitante vencedora, para fins de abertura de chamado técnico, obrigatoriamente as seguintes informações:
14.30.1 Código de fabricação ou número de série do equipamento se for o caso;
14.30.2 Anormalidade observada;
14.30.3 Nome do responsável pela solicitação;
14.30.4 Número do telefone para contato;
14.30.5 Número da Ordem de Serviço da EMBRATUR
14.31 Todas as solicitações feitas pela EMBRATUR serão registradas pela licitante vencedora para acompanhamento e controle da execução deste Contrato:
14.31.1 A licitante vencedora apresentara um Relatório de Visita contendo data e hora do chamado e do início e termino do atendimento, identificação do componente defeituoso, as providencias adotadas e demais informações pertinentes;
14.31.2 O Relatório deverá ser assinado pelo responsável pela solicitação de manutenção corretiva.
14.32 Se durante a vigência do contrato, houver a necessidade de alteração de algum componente da solução/software de Auditoria, o mesmo deverá ser apresentado, pela CONTRATADA, à critério da EMBRATUR, para avaliação técnica;
14.33 Para execução dos serviços de manutenção a licitante vencedora somente poderá desconectar os componentes de hardware ou desinstalar qualquer software que estiverem instalados ou ligados à solução/software de Auditoria com previa autorização da EMBRATUR;
14.34 A licitante vencedora deverá garantir que os meios de armazenamento magnéticos e/ou óticos utilizados pelos seus técnicos, durante as manutenções, estão livres de qualquer código malicioso ("vírus, worms, trojans ..."), voltado para a danificação ou degradação, tanto de dados, quanto de software ou hardware;

15. HABILITAÇÃO

15.1 Será considerada habilitada para participar do certame, além das exigências administrativas e legais especificadas no edital e neste Termo de Referência as empresas que apresentarem as seguintes documentações:
a) Declaração em papel timbrado da licitante de que prestará assistência técnica durante o período de garantia da solução/software de Auditoria propostos, e que mantêm rede de assistência técnica na região da entrega do produto e ainda, que prestará assistência técnica "on-site" para o objeto constante deste Termo de Referência.
b) Atestado ou declaração de capacidade técnica do licitante, fornecido por empresa pública ou privada que comprovem a venda, entrega, configuração e garantia mínima de 12 meses em software igual ao do objeto deste Termo de Referência e em quantidade igual ou superior a 50%.

PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

ANEXO II AO CONTRATO N. 034/2015 - CJF
PLANILHA DE PREÇOS

Lote	Descrição	Qtd	Valor Unitário	Valor Total
Item 1	Fornecimento do software com todas as características detalhadas para Microsoft Windows File Server	1	R$ 146.875,00	R$ 146.875,00
Item 2	Fornecimento do software com todas as características detalhadas para Microsoft Exchange Server	1	R$ 53.989,00	R$ 53.989,00
Item 3	Fornecimento do software com todas as características detalhadas para Microsoft Directory (AD)	1	R$ 119.975,00	R$ 119.975,00
Item 10	Serviços profissionais de implementação e testes para a solução	1	R$ 16.800,00	R$ 16.800,00
Item 11	Serviços profissionais de transferência de conhecimento da solução, por participante	2	R$ 8.500,00	R$ 17.000,00
Item 13	Serviços de garantia e suporte técnico (8x5) junto ao fabricante - software com todas as características detalhadas para Microsoft Windows File Server, pelo período de 36 (trinta e seis) meses	1	R$ 84.380,00	R$ 84.380,00
Item 14	Serviços de garantia e suporte técnico (8x5) junto ao fabricante - software com todas as características detalhadas para Microsoft Windows Exchange Server, pelo período de 36 (trinta e seis) meses	1	R$ 31.000,00	R$ 31.000,00
Item 15	Serviços de garantia e suporte técnico (8x5) junto ao fabricante - software com todas as características detalhadas para Microsoft Active Directory (AD), pelo período de 36 (trinta e seis) meses	1	R$ 67.890,00	R$ 67.890,00
Item 22	Serviços de Operação assistida, integração com novas versões do Windows e do Exchange e Estudos de caso	100	R$ 137,00	R$ 13.700,00
			Valor Total	**R$ 551.609,00**