



EDITAL DE LICITAÇÃO – SEF/MG

PREGÃO ELETRÔNICO Nº. 1191001- /2011

Processo nº: 0077447-1190-2010-4 SIGED: 11020-1190-2011

Tipo de Licitação: MENOR PREÇO

Lote Único

1 – PREÂMBULO

O **ESTADO DE MINAS GERAIS**, pela **SECRETARIA DE ESTADO DE FAZENDA**, realizará licitação na modalidade pregão eletrônico, em sessão pública, nos termos da Lei Estadual nº. 14.167, de 10 de janeiro de 2002, Decreto Estadual nº. 44.431, de 29 de dezembro de 2006, Decreto Estadual nº. 44.630, de 03 de outubro de 2007, Decreto Estadual 44.786, de 18 de abril de 2008, Decreto Estadual nº 44.998, de 03 de dezembro de 2008, Resolução Conjunta SEPLAG-SEDE-JUCEMG nº. 6419, de 30 de novembro de 2007, Resolução SEPLAG nº. 58, de 30 de novembro de 2007 e, subsidiariamente, pelas Leis Federais nº. 10.520, de 17 de julho de 2002 e nº. 8.666, de 21 de junho de 1993, e pelas condições estabelecidas no presente Edital, observados os preceitos da Lei Estadual nº. 13.994, de 18 de setembro de 2001.

Pregoeira: Martha Cristina de Oliveira Neves, MASP 326.517-0; Suplente: Marília Izabel de Almeida, MASP: 339.982-1; designadas por meio da Portaria SEF/SPGF Nº. 27, de 24/03/2011, Equipe de Apoio: Cláudia Ribeiro de Souza, MASP: 369.716-6, Eliana Mara Marcolino MASP: 363.129-8 e Alessandro Márcio de Moraes Zebral, MASP 340.218-7.

1.1 - A data e hora de abertura da sessão do pregão poderão ser consultadas no Portal de Compras/MG.

1.1.1 - Todas as referências de tempo no Edital, no aviso e durante a sessão pública, observarão obrigatoriamente o horário de Brasília - DF e, dessa forma serão registradas no sistema eletrônico e na documentação relativa ao certame.

1.2 - As propostas poderão ser enviadas após a disponibilização do Edital, exclusivamente por meio do sistema eletrônico, até a data e horário marcados para abertura da sessão, quando então encerrar-se-á automaticamente a fase de recebimento de propostas.

1.2.1 - O encaminhamento da proposta dentro do prazo previsto no subitem anterior é de responsabilidade exclusiva do fornecedor, o qual arcará com o ônus decorrente da perda de negócios diante da inobservância do horário fixado.

2 – OBJETO

Aquisição de uma solução de gerenciamento de identidades e de acessos, bem como *appliances* ou servidores para processamento da solução, contemplando licenças de uso, serviços de implantação, treinamento para capacitação de pessoal técnico da Superintendência de Tecnologia da Informação – STI/SEF, garantia dos *appliances* ou servidores e da ferramenta de gerenciamento de identidades e de acessos, como solução de provisionamento de usuários para os sistemas da SEF/MG, mediante Contrato, com o propósito de definir um padrão a ser adotado pelo poder Executivo do Estado de Minas Gerais, nas condições previstas neste Edital e seus anexos.



3 – DAS CONDIÇÕES DE PARTICIPAÇÃO

3.1 - Somente poderão participar da presente licitação as pessoas jurídicas do ramo pertinente ao objeto e desde que previamente credenciadas.

3.2 - Não poderão participar fornecedores que estiverem sob falência, recuperação judicial ou extrajudicial, concurso de credores, dissolução, liquidação, sociedades estrangeiras que não funcionem ou que não estejam autorizadas a operar no País, nem aqueles que tenham sido declarados inidôneos para licitar ou contratar com a Administração Pública ou punidos com suspensão do direito de licitar e contratar com a Administração Pública, e fornecedor da qual seja sócio, dirigente ou responsável técnico, qualquer servidor de órgão ou entidade pertencente ao Estado de Minas Gerais.

3.3 - A participação no certame implica aceitar todas as condições estabelecidas neste Edital.

3.4 - **O interessado em participar desta licitação, deverá, obrigatoriamente, realizar visita técnica, in loco,** às instalações do *datacenter* da SEF-MG, incluindo sua rede de computadores, sob gestão da Superintendência de Tecnologia da Informação – STI/SEF-MG, situado à Rua Alagoas, nº 880, bairro Funcionários, em Belo Horizonte – MG, para conhecer todos os aspectos pertinentes aos serviços a serem executados, bem como realizar a mensuração dos mesmos, bem como obter dados complementares que puderem ser fornecidos acerca do ambiente de Tecnologia da Informação e Comunicação - TIC da SEF/MG, visando à melhor formulação de sua proposta. Nessa ocasião, será fornecido o Termo de Visita Técnica, conforme modelo constante no subitem **7.4.4, alínea “f”**, documento indispensável a ser apresentado pelo fornecedor detentor da melhor oferta, durante a sessão do pregão.

3.4.1 - **A visita ocorrerá simultaneamente para todos os interessados em participar desta licitação**, 02 (dois) dias úteis antes da data fixada para abertura da sessão do pregão, ou seja, **no dia XX/XX/2011, às XX:XX horas**, e será comprovada por meio de “Termo de Visita Técnica”, expedido pela Diretoria de Infraestrutura e Operações – DIO/STI, que será condição de habilitação.

3.4.2. Os interessados deverão entrar em contato com a **STI/SEF/MG**, pelo telefone (031) 3217-6606, **diretamente com o Diretor da DIO/STI ou servidor por ele designado**, para confirmar a visita, a ser realizada no dia e horário definidos no item 3.4.1 acima com acompanhamento de servidor responsável ou indicado pela SEF/MG, momento em que o respectivo termo de visita deverá ser expedido.

3.4.3. A ausência do Termo de Visita Técnica na documentação de habilitação do licitante incorrerá na sua desclassificação do certame.

4 – DO CREDENCIAMENTO

4.1 - Para acesso ao sistema eletrônico, o fornecedor deverá credenciar-se no *site* **www.compras.mg.gov.br**, opção **“Cadastro de Fornecedores”**, no prazo mínimo de três dias úteis, antes da data da sessão do Pregão.

4.1.1 - Cada fornecedor deverá credenciar, no mínimo, um representante para atuar em seu nome no sistema, sendo que esse representante receberá uma senha eletrônica de acesso.

4.2 – O fornecimento da senha é de caráter pessoal e intransferível, sendo de inteira responsabilidade do fornecedor e de cada representante qualquer transação efetuada, não podendo ser atribuídos ao provedor ou ao gestor do sistema eventuais danos decorrentes do uso indevido da senha, ainda que utilizada indevidamente por terceiros.

4.2.1 - O fornecedor se responsabiliza por todas as transações realizadas em seu nome, assumindo como firmes e verdadeiras as propostas e os lances efetuados por seu



representante, sendo que o credenciamento do fornecedor implicará responsabilidade pelos atos praticados e a presunção de capacidade técnica para a realização das transações, sob pena da aplicação de penalidades.

4.3 - Informações complementares a respeito do credenciamento serão obtidas no *site* www.compras.mg.gov.br ou pela Central de Atendimento aos Fornecedores – LigMinas – telefone: 155 (para Capital ou cidades do interior de Minas Gerais) ou (31) 3303.7999 (para outras localidades e celular).

5 – DAS PROPOSTAS COMERCIAIS

5.1 - As propostas comerciais deverão ser enviadas, por meio do sítio www.compras.mg.gov.br, opção “Fornecedor”, nos termos do subitem 1.2 deste Edital, após preenchimento do formulário eletrônico.

5.1.1. As propostas para o objeto deste pregão deverão ser apresentadas de acordo com as especificações a que se refere o Anexo I deste Edital.

5.2 - O prazo de validade da proposta será de 60 (sessenta) dias.

5.3 – Os preços propostos deverão incluir todos os tributos, encargos sociais/trabalhistas, e quaisquer outros ônus que porventura possam recair sobre a execução do objeto, os quais ficarão, única e exclusivamente, a cargo do fornecedor.

5.4 - As propostas deverão apresentar preços unitários e total, por item e global para o lote único, em moeda corrente nacional, sendo vedada imposição de condições ou opções.

5.5 - A Microempresa e a Empresa de Pequeno Porte, optantes pelo Regime do *Simplex Nacional*, de que trata a Lei Complementar Federal nº.123, de 14 de dezembro de 2006, ficarão dispensadas de cumprir o disposto no subitem anterior.

5.6 - O fornecedor poderá concorrer ao Lote Único, objeto desta Licitação, desde que apresente cotação de preços para todos os itens relativos ao respectivo Lote, sob pena de ter sua proposta desclassificada.

6 – DA SESSÃO DO PREGÃO, DOS LANCES, DO JULGAMENTO DAS PROPOSTAS E DA DECLARAÇÃO DO VENCEDOR DO CERTAME.

6.1 - Da Sessão do Pregão e dos Lances

6.1.1 - Após análise e divulgação das propostas, o Pregoeiro fará o convite para que os fornecedores licitantes apresentem lances, desde que observados o horário estabelecido e as regras de aceitação.

6.1.2 - Na sessão pública, serão divulgadas, em tempo real, todas as mensagens trocadas no “chat” do sistema, inclusive valor e horário do menor lance registrado no sistema, vedada a identificação do fornecedor.

6.1.3 - Somente serão aceitos lances cujos valores forem inferiores ao último lance que tenha sido registrado no sistema.

6.1.4 – Alternativamente ao disposto no subitem anterior, o fornecedor poderá oferecer lance inferior ao último por ele ofertado e registrado no sistema.

6.1.5 - Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

6.1.6 - Caso o fornecedor não realize lances, permanecerá o valor da proposta apresentada para efeito da classificação final.



6.1.7 – Se houver desconexão com o Pregoeiro no decorrer da etapa competitiva do pregão, o sistema eletrônico poderá permanecer acessível aos participantes para a recepção de lances. O Pregoeiro, quando possível, dará continuidade, sem prejuízo dos atos realizados.

6.1.7.1 - Será suspensa a sessão do pregão se houver desconexão do sistema por tempo superior a 10 (dez) minutos, a qual será reiniciada após comunicação aos participantes.

6.1.8 - A etapa de lances da sessão pública será encerrada mediante aviso de fechamento iminente dos lances, emitido pelo sistema eletrônico, após o que transcorrerá período de tempo de 05 (cinco) até 30 (trinta) minutos, aleatoriamente determinado pelo sistema eletrônico, findo o qual será automaticamente encerrada a recepção de lances, sendo registrado no sistema o menor lance.

6.2 – Do Julgamento das Propostas

6.2.1 - O critério de julgamento será o de **MENOR PREÇO GLOBAL OFERTADO PARA O LOTE ÚNICO**.

6.2.2 – Será dado tratamento diferenciado e simplificado às microempresas e empresas de pequeno porte, desde que atendidas as condições estabelecidas no Decreto Estadual nº. 44.630, de 03 de outubro de 2007, na Resolução Conjunta SEPLAG-SEDE-JUCEMG nº. 6419, de 30 de novembro de 2007, e na Resolução SEPLAG nº. 58, de 30 de novembro de 2007.

6.2.3 – Será assegurada preferência ao fornecedor enquadrado como microempresa ou empresa de pequeno porte, como critério de desempate, nos termos dos artigos 44 e 45 da Lei Complementar nº. 123, de 14 de dezembro de 2006.

6.2.4 – Não obtidos lances, será verificada a conformidade entre a proposta de menor preço e o valor estimado da contratação.

6.2.5 – Se houver apenas uma proposta e desde que atendidas as condições previstas neste Edital, o Pregoeiro verificará se o preço encontra-se compatível com o valor estimado, apurado com base em pesquisas de mercado, podendo a proposta ser aceita.

6.2.6 – Aceita a proposta, o Sistema informará o detentor da melhor oferta, o qual deverá observar os requisitos de habilitação descritos no item nº. 7 deste Edital.

6.3 – Da Declaração do Vencedor

6.3.1 – Encerrada a etapa de lances e conferida a documentação relativa à habilitação, enviada pelo fax, o Pregoeiro encaminhará, pelo sistema eletrônico, contraproposta diretamente ao fornecedor que tenha apresentado o lance de menor valor, para que possa ser obtida melhor proposta, bem como decidir sobre a aceitação.

6.3.2 – O detentor da melhor proposta deverá encaminhá-la por escrito ao Pregoeiro, no prazo máximo de 02 (dois) dias úteis, a contar do encerramento da sessão, contendo o preço ofertado do objeto licitado, o nome do banco, o número da conta bancária e documentos da habilitação, para o seguinte endereço: Cidade Administrativa Tancredo Neves – Órgão: Secretaria de Estado de Fazenda – Prédio: Gerais – SPGF/DCOM/Divisão de Licitação - 6º andar; Ponto Focal: Diretoria de Compras – SGF/LICIT, situada na Rodovia Prefeito Américo Gianetti, s/n. Bairro Serra Verde, Edifício Gerais - CEP: 31630-901 - Belo Horizonte - Minas Gerais.

6.3.3 - Constatado o atendimento das exigências previstas no Edital, será declarado o vencedor ou, se a proposta não for aceita ou se o fornecedor não atender às condições de habilitação, serão convocados os demais fornecedores, na ordem de classificação, para exame dos documentos de habilitação.

6.3.4 – O licitante detentor da melhor oferta de preços estabelecido no Estado de Minas Gerais, após ser habilitado e declarado vencedor do certame, deverá adequar os valores da proposta comercial, discriminando os preços com o ICMS e os preços resultantes de sua dedução, em



decorrência da isenção do ICMS, conforme dispõe o item 136 da Parte 1 do Anexo I do Regulamento do ICMS, aprovado pelo Decreto Estadual nº. 43.080, de 13 de dezembro de 2002, e Resolução Conjunta SEF/SEPLAG nº. 3.458, de 22 de julho de 2003, alterada pela Resolução Conjunta SEF/SEPLAG nº. 4.264, de 21 de outubro de 2010, exceto o fornecedor optante pelo Simples Nacional, o qual deverá encaminhar a proposta pelo preço ofertado.

6.3.4.1 - Para a adjudicação e homologação do certame serão utilizados os valores com dedução do ICMS.

6.3.5 - Se o fornecedor, enquadrado na categoria de Microempresa ou Empresa de Pequeno Porte, for declarado vencedor, este deverá apresentar, durante a sessão do pregão, toda a documentação exigida neste Edital, inclusive os documentos relativos à regularidade fiscal, mesmo que a documentação apresente alguma restrição.

6.3.5.1 – Se houver restrição a respeito da regularidade fiscal da Microempresa e Empresa de Pequeno Porte, será concedido o prazo de dois dias úteis (prorrogáveis por igual período, a critério da Administração) para que haja regularização, pagamento ou parcelamento do débito e/ou emissão de certidões, cujo termo inicial será no momento em que o fornecedor for declarado vencedor.

6.3.5.2 - A não regularização no prazo previsto no subitem anterior, implicará decadência do direito à contratação, sem prejuízo das sanções previstas no artigo 81 da Lei nº. 8.666/93.

6.3.6 – O sistema gerará ata circunstanciada da sessão, na qual serão registrados todos os atos do procedimento e as ocorrências relevantes, disponível para consulta no site www.compras.mg.gov.br.

7 - DA HABILITAÇÃO

7.1 – Dos documentos comprobatórios da Habilitação Jurídica

- a) registro comercial para o empresário;
- b) ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades empresárias e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;
- c) inscrição do ato constitutivo, no caso de sociedades simples;
- d) decreto de autorização, em se tratando de sociedade estrangeira em funcionamento no País, acompanhada do ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

7.1.1 - Os documentos comprobatórios das alíneas “a”, “b” e “c” deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

7.2 – Dos documentos comprobatórios da Regularidade Fiscal:

- a) prova de inscrição no **Cadastro Nacional de Pessoas Jurídicas – CNPJ/MF**;
- b) prova de **regularidade para com a Fazenda Estadual do domicílio ou sede do fornecedor**;
 - b.1)** Se o fornecedor não estiver inscrito no cadastro de contribuintes do Estado de Minas Gerais, este deverá comprovar ainda a inexistência de débitos relativos a tributos estaduais em Minas Gerais, por meio de Certidão de Débitos Tributários - CDT, podendo ser solicitada pelo site www.fazenda.mg.gov.br.
- c) prova de **regularidade para com a Fazenda Municipal do domicílio ou sede do fornecedor**;
- d) prova de **regularidade para com a Fazenda Nacional**, por meio de Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União e Certidão Específica relativa a Contribuições Previdenciárias e Contribuições Devidas, Por Lei, a Terceiros, ambas fornecidas pela Secretaria da Receita Federal do Brasil;



e) certificado de **regularidade** perante o **Fundo de Garantia por Tempo de Serviço (FGTS)**, emitido pela Caixa Econômica Federal;

7.3 – Dos documentos comprobatórios da Qualificação Econômico-Financeira

a) **Balço patrimonial e as demonstrações contábeis do último exercício social**, exigíveis e apresentados na forma da lei, contendo a assinatura do contabilista responsável ou outro profissional equivalente, devidamente registrado no Conselho Regional de Contabilidade.

a.1) São considerados exigíveis na forma da lei o balanço patrimonial e as demonstrações contábeis, assim apresentados:

a.1.1) sociedades regidas pela Lei nº. 6.404/76 (sociedade anônima): os balanços publicados no Diário Oficial ou em jornal de grande circulação, bem como a fotocópia registrada ou autenticada na Junta Comercial da sede ou domicílio do fornecedor.

a.1.2) sociedades por cota de responsabilidade limitada e sociedades sujeitas ao regime estabelecido no Estatuto Nacional da Microempresa e Empresa de Pequeno Porte: a fotocópia do livro Diário (inclusive com os Termos de Abertura e de Encerramento, devidamente autenticado na Junta Comercial da sede ou domicílio do fornecedor ou em outro órgão equivalente) ou fotocópia do Balço e das Demonstrações Contábeis, devidamente registradas ou autenticadas na Junta Comercial da sede ou domicílio do fornecedor;

a.1.2.1) No caso de pequenas empresas optantes pelo Regime Simples Nacional, o balanço patrimonial poderá ser substituído pela Declaração de Imposto de Renda da Pessoa Jurídica do último Exercício;

a.1.3) sociedade criada no exercício em curso: a fotocópia do Balço de Abertura, devidamente registrado ou autenticado na Junta Comercial da sede ou domicílio.

a.1.4) O balanço patrimonial e as demonstrações contábeis poderão ser atualizados quando encerrados há mais de 3 (três) meses da data de apresentação da proposta, tomando como base a variação, ocorrida no período, do Índice Geral de Preços – Disponibilidade Interna - IGP-DI, publicado pela Fundação Getúlio Vargas - FGV ou de outro índice que o venha substituir, sendo vedada a substituição dos referidos documentos por balancetes ou balanços provisórios.

b) A **comprovação de se possuir, até a data da publicação do Edital, patrimônio líquido no valor mínimo de R\$ ()**, o que corresponde a aproximadamente 10% (dez por cento) do valor estimado para a contratação, na forma da lei, admitida a sua atualização para a data da respectiva licitação, através de índices oficiais;

c) **Certidão Negativa de Falência e recuperação judicial e extrajudicial**, expedida pelo cartório distribuidor da comarca da sede da pessoa jurídica, de acordo com o inciso II do artigo 31 da Lei nº. 8.666/93.

7.4 – Das demais disposições acerca da Habilitação

7.4.1 - O licitante que possuir o Certificado de Registro Cadastral – Cadastramento (CRC) emitido pela Unidade Cadastradora da Secretaria de Estado de Planejamento e Gestão – SEPLAG poderá apresentá-lo como substituto de documento dele constante, exigido para este certame, desde que o documento do CRC esteja com a validade em vigor.

7.4.2 - Na hipótese do subitem anterior, constando do CRC qualquer documento com o prazo de validade vencido, será assegurado ao fornecedor o direito de encaminhar o documento atualizado durante a sessão, via fax, no prazo máximo de 15 (quinze) minutos, após comunicação do Pregoeiro, concluindo-se nos 30 (trinta) minutos subsequentes.



7.4.3 – Serão analisados no Certificado somente os documentos exigidos neste certame.

7.4.4 - Juntamente com **todos** os documentos exigidos para habilitação, o detentor da melhor proposta, mesmo possuindo o CRC, deverá enviar via *fax*, durante a sessão, nos prazos definidos no subitem 7.4.2 os seguintes documentos, após comunicação pelo Pregoeiro:

a) Atestado(s) de capacidade técnica, fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, comprovando bom desempenho em serviços da mesma natureza, compatível com o objeto desta licitação, de forma satisfatória e a contento, devidamente datado(s) e assinado(s).

b) declaração de que possui recursos técnicos adequados e disponíveis para a execução dos serviços, objeto deste edital, sob pena de rescisão unilateral do contrato pela SEF/MG e da aplicação das sanções legais cabíveis, sem prejuízos das perdas e danos;

b.1) A declaração de que trata esta alínea deverá ser emitida pelo fornecedor, conforme modelo abaixo e assinada por quem possua poderes para representá-lo em juízo ou fora dele, comprovando-se esta condição:

DECLARAÇÃO

O fornecedor, com inscrição no CNPJ n.º,
sediado na, vem declarar, sob as penas da Lei, que possui recursos técnicos adequados para a execução dos serviços, objeto do Pregão Eletrônico n.º. 1191001 - / 2011, comprometendo-se a ter disponíveis, os seguintes requisitos mínimos:

- a)** equipe de profissionais qualificados para as atividades inerentes ao objeto desta licitação;
- b)** todos os equipamentos e softwares compatíveis e adequados para a realização dos serviços;
- c)** materiais/insumos necessários para a prestação dos serviços.

Data e local:

Nome empresarial do fornecedor:

Representante Legal:

Cargo

Assinatura do sócio procurador ou representante legal

Observação: esta declaração deverá ser emitida em papel que identifique o fornecedor.

- c)** declaração, conforme modelo abaixo, de que, na data prevista para a execução do contrato, os profissionais indicados para compor a equipe técnica pertencerão ao quadro permanente do fornecedor;



DECLARAÇÃO

O fornecedor, com inscrição no CNPJ n.º, sediado na, vem declarar, sob as penas da Lei, que na data prevista para a execução do contrato decorrente do Pregão Eletrônico n.º 1191001 - / 2011, os profissionais indicados para compor a equipe técnica pertencerão ao seu quadro permanente de funcionários

Data e local:

Nome empresarial do fornecedor:

Representante Legal:

Cargo

Assinatura do sócio procurador ou representante legal

Observação: esta declaração deverá ser emitida em papel que identifique o fornecedor.

c.1) a comprovação do vínculo de natureza permanente dos profissionais que comporão a equipe técnica com o fornecedor far-se-á: se empregado, através da cópia da carteira de trabalho e previdência social – CTPS, ou equivalente; se diretor ou sócio da empresa, através do ato de investidura do cargo ou cópia do Contrato Social; se prestador de serviços, através de contrato regido pela legislação civil comum.

d) Declaração assinada por quem possua poderes para representá-lo em juízo ou fora dele:

DECLARAÇÃO

Declaro, para os devidos fins, sob as penas da lei, que as informações abaixo sobre o fornecedor _____, CNPJ/MF n.º _____, são firmes e verdadeiras:

1. inexistência de trabalho noturno, perigoso ou insalubre por menores de 18 (dezoito) anos ou a realização de qualquer trabalho por menores de 16 (dezesseis) anos, salvo na condição de aprendiz, na forma da lei;
2. até a presente data, todas as informações constantes da base de dados do Cadastro Geral de Fornecedores do Portal de Compras do Estado de Minas Gerais são verdadeiras e exprimem a atual situação do fornecedor, comprovada pelos documentos apresentados ao setor de cadastramento de fornecedores;
3. o enquadramento ao disposto no art. 3º da Lei Complementar Federal n.º. 123, de 14 de dezembro de 2006 (**aplicável somente para ME e EPP**);
4. sob as penas da Lei, na forma do § 2º, artigo 32, da Lei 8.666/93 e suas alterações posteriores, que, até a presente data, não existem fatos supervenientes e impeditivos para sua participação no Pregão Eletrônico 1191001 /2011, da Secretaria de Estado de Fazenda de Minas Gerais e que não pesa contra si declaração de inidoneidade expedida por Órgão da Administração Pública de qualquer esfera de Governo.

Declaro, ainda, o compromisso de informar formalmente ao CAGEF a ocorrência de qualquer fato impeditivo posterior a esta declaração que interfira nos dados constantes dos registros cadastrais do Estado de Minas Gerais, inclusive em relação ao porte do fornecedor declarado acima.

Data e local:

Assinatura do representante legal

Obs: esta declaração deverá ser emitida em papel que identifique o fornecedor



e) Documento hábil à comprovação da opção pelo Regime do *Simples Nacional* (**aplicável somente no caso do detentor da melhor oferta ser fornecedor mineiro optante pelo Regime *Simples Nacional***).

f) “**Termo de Visita Técnica**”, que será expedido pela Diretoria de Infraestrutura e Operações – DIO/STI, nos seguintes termos:

TERMO DE VISITA TÉCNICA

Atestamos, para fins de participação no Pregão Eletrônico n.º **1191001 /2011**, processo n.º **0077447-1190-2010-4**, da Secretaria de Estado de Fazenda de Minas Gerais, que o fornecedor _____, com inscrição no CNPJ n.º _____, por intermédio do seu representante Sr.(a) _____, examinou as instalações do *datacenter* da SEF-MG, inclusive sua rede de computadores, sob gestão da Superintendência de Tecnologia da Informação – STI/SEF-MG, situado à Rua Alagoas, n.º 880, Bairro Funcionários, em Belo Horizonte – MG, conhecendo todos os aspectos pertinentes aos serviços a serem executados, bem como realizando a mensuração dos mesmos.

Data e local:

Diretoria de Infraestrutura e Operações – DIO/STI– Nome/Masp

g) Descrição da solução técnica ofertada, bem como manuais destinados a comprovar sua adequação dessa solução às especificações técnicas contidas no Anexo I deste Edital, devendo ser informado, para cada item e subitem da especificação, o produto ofertado pelo fornecedor que permite atender ao referido item, bem como o manual e a página do manual que permitem comprovar esse atendimento.

7.4.5 - Todos os documentos apresentados para habilitação deverão conter, de forma impressa, preferencialmente, o nome empresarial, o endereço e o CNPJ do fornecedor.

7.4.5.1 - Se o fornecedor figurar como estabelecimento matriz, todos os documentos deverão estar em nome da matriz; se filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, tenham que ser emitidos, obrigatoriamente, em nome da matriz.

7.4.6 – Será inabilitado o fornecedor que deixar de apresentar quaisquer dos documentos exigidos para a habilitação ou apresentá-los em desacordo com o Edital.

7.4.7 - A SEF/MG reserva-se o direito de conferir as informações prestadas por meio de consultas e visitas às emitentes dos atestados e declarações.

7.4.8 – Declarações falsas sujeitarão o fornecedor às sanções previstas na legislação em vigor.

7.4.9 - Para fins de habilitação, a verificação em sítios oficiais de órgão e entidades emissores de certidões constitui meio legal de prova, sendo que a ausência de qualquer documento de habilitação passível de consulta, durante a sessão, por sistema eletrônico, não acarretará a inabilitação do fornecedor, devendo os documentos objetos de consulta serem juntados ao processo pelo pregoeiro.

7.4.10 – Poderá ser consultada a regularidade fiscal do fornecedor e providenciada a impressão dos documentos comprobatórios, inclusive em relação à comprovação dos registros e alterações societárias realizados em nome do fornecedor perante a Junta Comercial.

7.4.11 – Se ocorrer desconexão do sistema durante consulta da documentação pelo sistema eletrônico e não sendo enviada a documentação atualizada via fax, nos prazos definidos no subitem 7.4.2, o fornecedor será inabilitado.



7.4.12 - Os documentos provenientes da *Internet* terão sua autenticidade certificada junto aos sites dos órgãos emissores para fins de habilitação.

8 - DOS RECURSOS

8.1 - Declarado o vencedor, o participante do certame terá até 10 minutos para manifestar imediata e motivadamente, exclusivamente por meio do sistema eletrônico, em campo próprio, a intenção de recorrer, sendo concedido o prazo de três dias úteis, contados da sessão do pregão, para apresentação das razões de recurso, ficando os demais participantes, desde logo intimados, sem necessidade de publicação, a apresentarem contrarrazões em igual número de dias, contados do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos.

8.1.1. Todos procedimentos para interposição de recurso, compreendida a manifestação da intenção do licitante durante a sessão pública, e o encaminhamento das razões do recurso e de eventuais contrarrazões pelos demais licitantes, serão realizados exclusivamente por meio do sistema eletrônico, em formulários próprios;

8.1.2 a apresentação de documentos complementares, devidamente identificados, relativos aos recursos interpostos ou contrarrazões, se houver, será efetuada, mediante documento protocolizado junto ao Setor de Protocolo, localizado na Cidade Administrativa Tancredo Neves – Órgão: Secretaria de Estado de Fazenda – Prédio: Gerais – SGF/DCOM/Divisão de Licitação - 6º andar; Ponto Focal: Diretoria de Compras – SGF/LICIT, situada na Rodovia Prefeito Américo Gianetti, s/n. Bairro Serra Verde, Edifício Gerais - CEP: 31630-901 - Belo Horizonte - Minas Gerais, observados os prazos previstos no item 8.1.

8.2 - Não serão conhecidos recursos não registrados na forma e prazo estabelecidos no item 8.1 do edital, além de que, a falta de manifestação imediata e motivada do fornecedor, importará decadência do direito de recurso.

8.3 - Os recursos serão decididos no prazo de 05 (cinco) dias úteis, contados do encerramento do prazo para apresentação de contrarrazão, sendo que o acolhimento de recurso importará validação exclusivamente dos atos suscetíveis de aproveitamento.

8.4 - A decisão do recurso será divulgada no sítio eletrônico www.compras.mg.gov.br, no campo quadro de avisos do referido pregão, comunicado à licitante que o interpuser via fac-símile ou e-mail e publicada no Diário Oficial do Estado, “Minas Gerais”, no Caderno I, Diário do Executivo, item Editais e Avisos.

9 - DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

9.1 - Inexistindo manifestação recursal, o Pregoeiro adjudicará o objeto da licitação ao vencedor do certame, com a posterior homologação do resultado pela autoridade competente.

9.2 - Decididos os recursos, porventura interpostos, e constatada a regularidade dos atos procedimentais, a autoridade competente adjudicará o objeto ao vencedor e homologará o procedimento licitatório.

9.2.1 - A adjudicação e homologação do objeto ao vencedor estarão, a critério da Administração, condicionadas ao recebimento de Termo de Aprovação, decorrente da realização de Prova de Amostra, visando à verificação de conformidade entre a solução ofertada e as especificações deste Edital e anexos, de acordo com o item 3 do Anexo I deste Edital.

10 – DO CONTRATO

10.1 - Declarado o vencedor, com resultado homologado, este será convocado a celebrar contrato,



nos termos da minuta que integra este Edital, Anexo IV, devendo o instrumento ser assinado e devolvido no prazo máximo de 05 (cinco) dias, a contar da data de recebimento do ofício convocatório.

10.1.1. No ato de assinatura do contrato deverão ser apresentados todos os documentos exigidos neste Edital, caso estejam vencidos.

10.2 – Se o fornecedor, adjudicatário do objeto do certame, não apresentar situação regular no ato de assinatura do contrato ou recusar sua celebração, serão convocados os fornecedores remanescentes do certame, observada a ordem de classificação.

10.3 – Eventual solicitação de prorrogação do prazo para assinatura do contrato somente poderá ser apresentada, devidamente fundamentada, antes do decurso do prazo previsto no subitem 10.1.

10.4 - A recusa injustificada do adjudicatário em assinar o contrato no prazo estabelecido no subitem 10.1 caracterizará o descumprimento total da obrigação assumida, ficando o mesmo sujeito à multa de 10% (dez por cento) do valor do contrato, atualizado monetariamente pelo IPCA, que deverá ser quitada no prazo de 10 (dez) dias, contados da data do recebimento da notificação.

10.5 – Para fins de pagamento, o fornecedor deverá informar domicílio bancário junto ao Banco do Brasil S.A., nos termos da Portaria nº 001, de 9/11/2010, do Diretor da Superintendência Central de Administração Financeira da Secretaria de Estado de Fazenda de Minas Gerais – SCAF/SEF.

10.5.1 - Caso o fornecedor não tenha conta no banco a que se refere o subitem 10.5, deverá providenciar a abertura de conta corrente em qualquer agência do referido banco, comunicando à SEF-MG os dados de seu domicílio bancário para fins de certificação de cadastro junto ao Sistema Integrado de Administração Financeira – SIAFI/MG e posterior recebimento de seus créditos.

10.5.2 - Excepcionalmente, mediante manifestação formal do fornecedor que esteja impossibilitado de manter conta corrente junto ao Banco do Brasil, o pagamento poderá ser feito nos termos do § 2º do art. 1º da Portaria nº 001/2010.

11 - DAS SANÇÕES ADMINISTRATIVAS

11.1 – Na forma prevista no art. 12 da Lei nº.14.167, de 2002, garantida a ampla defesa, poderá ser aplicada sanção de impedimento de licitar e contratar com órgãos e entidades da Administração Estadual, àquele licitante que:

- a) apresentar documentação falsa;
- b) deixar de apresentar documentação exigida para o certame;
- c) ensejar o retardamento da execução do objeto da licitação;
- d) não mantiver a proposta;
- e) falhar ou fraudar a execução do futuro contrato;
- f) comportar-se de modo inidôneo; ou
- g) cometer fraude fiscal.

11.2 - O prazo do impedimento de licitar e contratar será de até cinco anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade.

11.3 - As sanções serão obrigatoriamente registradas no CAFIMP, devendo o licitante ser descadastrado junto ao Cadastro de Fornecedores do órgão ou entidade promotora da licitação, por igual período, sem prejuízo das multas e das demais cominações legais previstas no contrato.

12 - DAS DISPOSIÇÕES GERAIS



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

12.1 - Este Edital deverá ser interpretado na íntegra e após o encaminhamento da proposta, não serão aceitas alegações de desconhecimento ou discordância de seus termos.

12.2 - A presente licitação somente poderá ser revogada por razão de interesse público, decorrente de fato superveniente e comprovado, ou anulada, no todo ou em parte, por ilegalidade, de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado.

12.3 - O Pregoeiro, no interesse da Administração, poderá relevar omissões puramente formais observadas na documentação e proposta, desde que não contrariem a legislação vigente e não comprometam a lisura da licitação, sendo permitido ao Pregoeiro ou Autoridade Superior promover qualquer diligência destinada a esclarecer ou a complementar a instrução do processo, bem como solicitar aos órgãos competentes a elaboração de pareceres técnicos destinados a fundamentar as decisões.

12.4 - Caberá ao fornecedor credenciado acompanhar as operações no sistema eletrônico durante a sessão pública do pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo Pregoeiro, pelo sistema ou de sua desconexão.

12.5 - Informações complementares que visem obter maiores esclarecimentos sobre a presente licitação poderão ser solicitadas ao Pregoeiro até 2 (dois) dias úteis anteriores à data fixada para recebimento das propostas, no horário de 08:00 às 11:00 horas e de 13:00 às 17:00 horas, de segunda a sexta-feira, pelo fax (31) 3915-6411 ou pelo e-mail: spgfdcomlicitacao@fazenda.mg.gov.br.

12.5.1. Nos pedidos de maiores esclarecimentos, os interessados deverão se identificar (CNPJ, Nome Empresarial e nome do representante legal), bem como informar os dados para contato (endereço completo, telefone, fax e e-mail).

12.6 – Até 2 (dois) dias úteis anteriores à data fixada para recebimento das propostas, qualquer pessoa, inclusive licitante, poderá impugnar o ato convocatório, mediante documento protocolizado junto ao Setor de Protocolo, localizado na Cidade Administrativa Tancredo Neves – Órgão: Secretaria de Estado de Fazenda – Prédio: Gerais – SGF/DCOM/Divisão de Licitação - 6º andar; Ponto Focal: Diretoria de Compras – SGF/LICIT, situada na Rodovia Prefeito Américo Gianetti, s/n. Bairro Serra Verde, no Município de Belo Horizonte /MG - CEP: 31630-901.

12.7- Na contagem dos prazos estabelecidos neste edital exclui-se o dia do início e inclui-se o do vencimento, e consideram-se os dias consecutivos. Só se iniciam e expiram os prazos em dia de expediente neste Órgão. Para definição dos dias úteis nos períodos citados neste Edital, deverá ser considerado o calendário adotado pelo Governo do Estado de Minas Gerais.

12.8 - Os fornecedores que retirarem o Edital pela *Internet*, deverão enviar os dados cadastrais para o seguinte e-mail: spgfdcomlicitacao@fazenda.mg.gov.br.

Belo Horizonte, de de 2011.

ARIANA APARECIDA GONÇALVES PEREIRA DE CARVALHO
Superintendente de Gestão e Finanças



ANEXO I - TERMO DE REFERÊNCIA

PREGÃO ELETRÔNICO N.º. 1191001 /2011

Processo nº. 0077447-1190-2010-4 – SIGED : 00011020-1191-2011

1 – DO OBJETO:

1.1 - Aquisição de uma solução de gerenciamento de identidades e de acessos, bem como *appliances* ou servidores para processamento da solução, contemplando licenças de uso, serviços de implantação, treinamento para capacitação de pessoal técnico da Superintendência de Tecnologia da Informação – STI/SEF, garantia dos *appliances* ou servidores e da ferramenta de gerenciamento de identidades e de acessos, como solução de provisionamento de usuários para os sistemas da SEF/MG, mediante Contrato, com o propósito de definir um padrão a ser adotado pelo poder Executivo do Estado de Minas Gerais,, mediante Contrato, nas condições previstas neste Edital e seus anexos.

1.2 - DAS ESPECIFICAÇÕES TÉCNICAS DO OBJETO

Aquisição de uma solução de gerenciamento de identidades e de acessos, composta dos seguintes produtos e serviços:

- a) Licenças de uso de uma solução de software para gerenciamento de identidades e de acessos, como solução de provisionamento de usuários para os sistemas da SEF/MG, bem como *appliances* ou servidores para processamento da solução.
 - a.1) A oferta do fornecedor deverá atender integralmente às especificações técnicas apresentadas neste Termo de Referência.
- b) Serviços de implantação da solução conforme especificados no subitem 1.2.2 deste Termo de Referência.
- c) Serviços de treinamento para capacitação de pessoal técnico, indicado pela SEF-MG, na configuração, manutenção e uso das ferramentas envolvidas na solução, conforme especificados no subitem 1.2.4 deste Termo de Referência.
- d) Garantia dos *appliances* (se aplicável) e da ferramenta conforme especificados no subitem 1.2.5 deste Termo de Referência.

LOTE ÚNICO			
AQUISIÇÃO DE SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADES E DE ACESSOS			
Item	Descrição	Quant.	Prazo de Entrega
1	Fornecimento de hardware (<i>appliances</i> ou servidores) para compor a solução de gerenciamento de identidades e de acessos.	1	90 (noventa) dias contados da assinatura do contrato.
2	Fornecimento de software (licenças de uso) para compor a solução de gerenciamento de identidades e de acessos baseada	1	90 (noventa) dias contados da assinatura do contrato.
3	Serviços de implantação da solução	1	240 (duzentos e quarenta) dias contados da assinatura do contrato.



4	Serviços de treinamento para capacitação de pessoal técnico (aproximadamente 174 treinandos) indicado pela SEF-MG, na configuração, manutenção e uso das ferramentas envolvidas na solução.	1	300 (trezentos) dias contados da assinatura do contrato.
5	Garantia dos <i>appliances</i> ou servidores e da ferramenta de software para gerenciamento de identidades e de acessos, incluindo manutenção pelo prazo de 48 meses, bem como o fornecimento de novos releases e versões e suporte técnico na modalidade 24 X 7 pelo período de 48 meses.	1	Imediatamente, após a expedição do Termo de Aceite Técnico relativo ao item 3.
6	Horas de serviço de <i>coaching/mentoring</i>	1000	Sob demanda, após a expedição do Termo de Recebimento a que se referem os itens 1 e 2 acima

1.2.1 - ESPECIFICAÇÃO DA SOLUÇÃO

A solução de software de gerenciamento de identidades e acessos deve apresentar as seguintes características básicas:

- I. A solução deve se apresentar através de produto único ou composto por módulos, sendo necessário, nesse caso, que cada módulo seja totalmente integrado com os demais e que nenhuma funcionalidade requisitada dependa de sistemas ou módulos comercializados como software de prateleira por terceiros, sendo admitida a elaboração de programas pelo fornecedor como parte do esforço de customização, sempre que essa possibilidade for expressamente permitida nas especificações.
- II. A solução deve apresentar interface de usuário totalmente nativa em língua portuguesa, variação regional do Brasil, incluindo nome de ações, informações e ajuda. A interface de ajuda ou *help on-line* poderá ser em língua inglesa, mas deverá permitir a customização nativa (funcionalidade nativa customizada) ou tradução..
- III. A solução deve apresentar interface de uso através de aplicativos baseados em páginas para execução em navegadores web.
- IV. A solução deve fazer comunicação segura entre clientes e servidores através de criptografia de dados realizada com os algoritmos previstos nos protocolos Transport Layer Security (TLS) ou Secure Socket Layer (SSL).
- V. A solução deve apresentar interface gráfica do usuário, ou seja, deve permitir a gestão completa dos ciclos de vida dos seguintes itens, tornando-os totalmente funcionais e aplicáveis, sem a necessidade de programação (edição de linhas de código escrito):
 - a) identidades digitais;
 - b) perfis de acesso;
 - c) fluxos de aprovação;
 - d) políticas de controle de acesso;
 - e) formulários de solicitação.
- VI. A solução deve ser nativamente integrável, interoperável e compatível com as seguintes tecnologias, em termos de execução e de troca de dados:
 - Nas estações de trabalho clientes, com os sistemas operacionais Microsoft Windows XP, Microsoft Windows Vista e Windows 7;
 - Nos servidores, com as seguintes plataformas:
 - a) serviços de diretórios:



- a.1) Microsoft Active Directory (AD), versão 2003 ou superior.
- a.2) Repositórios LDAP v3.

b) sistemas operacionais:

- b.1) Red Hat Enterprise Linux AS.
- b.2) Microsoft Windows 2000 Server e Microsoft Windows 2003 Server em todas as suas distribuições.
- b.3) SUN Solaris 10.

c) Banco de dados:

- c.1) SGBD ORACLE, versão 10G ou superior.
- c.2) MS SQL Server 2005 ou superior.

d) Software de correio eletrônico:

- d.1) Microsoft Exchange Server 2007 ou superior.

e) Suporte a SPML (Service Provisioning Markup Language);

f) Plataforma Java (Java SE Development Kit (JDK) 5.0 ou superior e J2EE SDK 1.4 ou superior).

VII. Os dados das identidades e perfis, workflows e políticas, bem como os metadados necessários e as informações de registro histórico do ciclo de vida dos objetos geridos devem ser armazenados em um repositório estruturado e centralizado.

- a) O repositório central deve sincronizar as informações nele contidas com os repositórios (AD, LDAP, Unix etc.) da solução, bem como com os repositórios dos sistemas integrados, de forma automatizada e de acordo com prazos ou eventos estabelecidos. A sincronização deve acontecer de forma bidirecional para os casos a serem definidos pela SEF/MG, não importando a origem do evento dela demandante.
- b) O sistema deve permitir a gerência das identidades e dos perfis sem necessidade de que os sistemas integrados estejam ativos ou *on-line*, desde que garantida a sincronização dos dados após o sistema voltar a ficar *on-line*.
- c) A solução de gerência de identidades deverá ter alta disponibilidade, com redundância de todos os seus componentes críticos.
- d) Sem prejuízo do atendimento do requisito de alta disponibilidade estabelecido na alínea c) acima, a solução não deve afetar o funcionamento das aplicações por ela provisionadas quando ficar indisponível.

VIII. A solução deverá disponibilizar interfaces por meio de serviços seguros que permitam a integração de sistemas existentes, possibilitando a esses sistemas efetuarem operações de provisionamento e consulta, empregando para esse fim:

- a) Web Services;
- b) Java.

IX. A solução deve permitir a implementação e a utilização de políticas de integração dos sistemas aplicativos, de modo independente em cada aplicação integrada.

X. A solução deve permitir a interação com aplicativos externos para a avaliação e execução de políticas de integração, por meio de:

- a) Web Services;
- b) Java.



- XI. A solução deve apresentar uma interface ou ferramenta própria para as tarefas administrativas como, por exemplo: definição de *workflows*, desenvolvimento dos conectores, notificações e alertas do sistema e extração de relatórios.
- XII. A solução deve ser totalmente redimensionável, ou seja, deve suportar quaisquer quantidades dos diversos tipos de objetos suportados, tais como identidades, perfis, fluxos de trabalhos e demais metadados.
- XIII. A solução deve permitir a importação de dados de usuário, roles, perfil e recursos através de arquivos texto, csv, tabelas ou outro formato/meio para a realização de carga de dados em seu repositório, permitindo sincronização automática desses dados após finalização da operação manual..
- XIV. A solução deve ser flexível, respeitadas as suas compatibilidades funcionais, permitindo a evolução dos sistemas integrados e agregação de outros.
- XV. A solução deve possuir ajuda *on-line* em qualquer ponto do sistema para o usuário final. Deverá também disponibilizar ajuda *on-line* e/ou manual em outro formato para toda a parte administrativa da solução.
- XVI. A arquitetura da solução deve possuir mecanismo de alta disponibilidade e balanceamento de cargas nas camadas de interface, aplicação e repositório – *backup e restore*.
- XVII. A arquitetura da solução deve possuir mecanismo de cópia de segurança e restauração de todos os dados de seu repositório – *backup e restore*.
- XVIII. A arquitetura da solução deve possuir mecanismo de recuperação de seu ambiente de instalação e configuração (*backup e restore*) ou permitir que se faça uma reinstalação, quando não for possível a recuperação, sem a necessidade de se efetuar carga de repositório de dados.
- XIX. A arquitetura da solução deve possuir sistema de contingência capaz de restaurar completamente o conteúdo do sistema de produção a partir do backup, tornando-o completamente operacional.
- XX. A solução deve ser capaz de operar de forma integrada e síncrona com diversos controladores de domínio de redes.
- XXI. A solução deve suportar nativamente ou através de customizações nativas (funcionalidade nativa customizada) ou pontos de extensão os seguintes modelos de reconciliação de identidades::
- a) Reconciliação de identidades com origem confiável. Neste modelo de reconciliação, todos os atributos das identidades sincronizadas com a solução de gestão de identidades são criados e mantidos por um único repositório, também conhecido como sistema de origem.
 - b) Reconciliação de identidades com múltiplas origens confiáveis. Neste modelo de reconciliação, os atributos das identidades sincronizadas com a solução de gestão de identidades são criados e mantidos por mais de um repositório. Cada atributo de identidade é vinculado a um repositório específico.
 - c) Reconciliação total de identidades. Neste modelo de reconciliação, todas as identidades de um repositório, independentemente de quaisquer eventos de criação, atualização ou exclusão, são sincronizadas com a solução de gestão de identidades.
 - d) Reconciliação total de identidades dividida em lotes. Neste modelo de reconciliação, todas as identidades de um repositório, independentemente de quaisquer eventos de criação, atualização ou exclusão, são sincronizadas com a solução de gestão de identidades, sendo possível dividir o número total de identidades sincronizadas em lotes de processamento com tamanho máximo pré-determinado. Para esta modalidade reconciliação, será admitida a possibilidade de extração dos dados do repositório em *batch*.



- e) Reconciliação incremental de identidades. Neste modelo de reconciliação, somente as identidades que sofreram eventos de criação, atualização ou exclusão, depois de determinada unidade de tempo, são sincronizadas com a solução de gestão de identidades. Para esta modalidade reconciliação, será admitida a possibilidade de extração dos dados do repositório em *batch*.
- f) Reconciliação incremental de identidades com filtro. Neste modelo de reconciliação, somente as identidades que sofreram eventos de criação, atualização ou exclusão, depois de determinada unidade de tempo, e cujos atributos se enquadrem em determinada condição, são sincronizadas com a solução de gestão de identidades. Para esta modalidade reconciliação, será admitida a possibilidade de extração dos dados do repositório em *batch*.
- g) Reconciliação de identidades com acionamento agendado. Neste modelo de reconciliação, o processo de sincronização entre os repositórios de identidades e a solução de gestão de identidades é disparado de acordo com o horário e a frequência pré-estabelecidos. Também deve ser possível estabelecer a quantidade máxima de tentativas em caso de erro de execução.
- h) Reconciliação de recursos com acionamento agendado. Neste modelo de reconciliação, a descrição dos recursos (grupos, papéis, perfis, privilégios e funcionalidades) de um determinado repositório é sincronizada com a solução de gestão de identidades, de acordo com o horário e a frequência pré-estabelecidos. Também deve ser possível estabelecer a quantidade máxima de tentativas em caso de erro de execução.

- XXII. A solução deve oferecer serviço de diretório baseado em padrões de mercado LDAP v2 e v3, modelo X.500, com conexão segura.
- XXIII. A solução deve permitir configurações de alta disponibilidade e possuir mecanismos de monitoramento do desempenho..
- XXIV. A solução deve prover uma visão unificada de usuários buscando informações em seu repositório, mesmo que os dados estejam armazenados em repositórios distintos e gerenciados pela solução, como servidores ou árvores LDAP, sem a necessidade de sincronizar ou replicar diretórios para se efetuar esta gestão.
- XXV. A solução deve possuir recursos de auto-otimização de forma dinâmica nos *pools* de conexões com banco de dados ou conjuntos de *threads* que servem as aplicações do servidor de aplicações, de forma a otimizar o uso de recursos de acordo com a demanda das aplicações..
- XXVI. A solução deve expor as informações dos usuários através de serviços LDAP e DSML.
- XXVII. A solução a ser contratada deverá atender aos seguintes requisitos de gestão de identidade:
 - a) possuir recurso que permita criar integração com sistemas de controles de usuários (servidores efetivos, prestadores, estagiários) para automatizar ações como:
 - a.1) criação automática de identidades com perfis adequados;
 - a.2) exclusão automática, desativação em caso de desligamento ou reativação de identidades;
 - a.3) criação ou alteração automática de identidades, sempre que houver alteração nos atributos da mesma; nesse caso, deve-se aplicar a sincronização cabível e executar os procedimentos estabelecidos de acordo com as regras de negócio, incluindo o início automático de fluxo de aprovação, se necessário;
 - a.4) bloqueio e desbloqueio automático de identidades em caso de eventos de férias, licenças, entre outros;
 - b) prover formulários web para criação e modificação de identidades;



- c) prover acessos automáticos às identidades, em caso de novas aplicações serem adicionadas ao perfil relacionado;
 - d) suportar definição de perfis de acesso que agrupem diferentes privilégios de múltiplos sistemas e plataformas;
 - e) permitir que uma identidade possua múltiplos perfis;
 - f) possuir definição de perfis hierárquicos, permitindo que os perfis de acesso sejam associados a uma representação de uma estrutura hierárquica organizacional;
 - g) permitir que alterações nas permissões de um determinado perfil sejam automaticamente replicadas às identidades conectados a este perfil;
 - h) prover perfis e privilégios às identidades de acordo com atributos como, por exemplo, função, setor, entre outros.
- XXVIII.** A solução deve permitir a importação e consolidação dos dados das identidades previamente existentes nos sistemas integrados para seu próprio repositório, e deve permitir que essa importação seja feita de forma parcial e parametrizada.
- XXIX.** A solução deve propagar as informações de cada identidade para os repositórios de dados de cada sistema integrado, incluindo alterações de senha e ativações e desativações de contas, mantendo-os sincronizados e atualizados automaticamente, sem intervenção humana, durante sua operação normal.
- XXX.** A sincronização de identidades deve suportar a associação de identidades criadas na própria solução com identidades existentes nos sistemas integrados, fazendo as verificações necessárias a fim de não permitir replicação indevida.
- XXXI.** A solução deve permitir a definição dos sistemas que são donos/destinatários dos atributos específicos de contexto das identidades digitais, quando necessários, de forma gráfica, podendo-se realizar transformações de dados através de customizações ou scripts de programação.
- XXXII.** A solução deve permitir a atribuição e o registro automático de datas relevantes ao ciclo de vida das identidades.
- XXXIII.** A solução deve permitir a sincronização de identidades, levando em conta:
- a) grupos e perfis;
 - b) quaisquer outros objetos ligados ao usuário e grupos, tais como dados complementares do usuário, restrições (unidade administrativa, regional, etc.) e exceções.
- XXXIV.** A solução deve permitir que as políticas ou regras definidas tenham a capacidade de reutilização entre as aplicações integradas ao repositório de identidades.
- XXXV.** A solução deve ter a capacidade de permitir o autorregistro de usuários baseado em políticas de autorização e regras de negócio associadas.
- XXXVI.** A solução deve permitir a elaboração e utilização de regras e políticas para a definição e criação de nomes de usuários, *usernames*, *logins* ou identificadores das identidades digitais, sem restrições quanto a tamanhos e símbolos utilizados.
- XXXVII.** A solução deve ser compatível com a API Java Regex para permitir a elaboração de regras de formação do nome de usuário, a partir de atributos do mesmo.



- XXXVIII.** A solução deve permitir a requisição e a troca do *username*, *login* ou nome de usuário de uma identidade, sem afetar o registro histórico de ações dessa identidade e sem causar a perda ou alteração de qualquer outro atributo.
- XXXIX.** A solução sempre deve verificar a não existência de um identificador gerado ou sugerido antes de atribuí-lo a uma nova identidade, ou a uma identidade que solicite troca do mesmo.
- XL.** A solução deve permitir a exclusão lógica de identidades desativadas/desabilitadas pelos administradores, desde que completamente registrada a operação.
- XLI.** A solução deve permitir a sincronização de identidades entre os diversos sistemas integrados, mesmo que nesses sejam usados identificadores ou nomes de usuário ou *logins* distintos.
- XLII.** A solução deve permitir o agendamento de ações relacionadas às identidades digitais, como criação, desativação, suspensão, reativação e alteração de atributos.
- XLIII.** A solução deve permitir a criação e execução de regras de ausência temporária, por motivos de férias ou licença dos usuários titulares das identidades digitais, como suspensão ou restrição dos acessos, de acordo e em sincronia com eventos e dados geridos pela Superintendência de Recursos Humanos da SEF/MG.
- XLIV.** A solução deve permitir que conjuntos mínimos de privilégios sejam estipulados, mesmo que através de perfis, e que possam ser atribuídos às identidades criadas nos repositórios dos sistemas integrados, isolada ou combinadamente, conforme regras de negócios e valores dos atributos das identidades, mesmo sem ter seguido nenhum fluxo de aprovação.
- XLV.** A solução deve permitir a configuração para delegação de privilégios de operação, baseada em perfis, como solicitação da criação de nova identidade, solicitação de adição de perfil ou de recurso específico, entre outros.
- XLVI.** A solução deve permitir que qualquer sistema integrado inicie uma atividade de provisionamento e deve enquadrá-la, automaticamente, no fluxo de aprovação adequado, segundo as regras de negócio.
- XLVII.** A solução deve permitir que sistemas sejam cadastrados e listados como recursos através de conectores, extensões, acesso ao banco de dados do sistema, API, e que um conjunto mínimo de ações automatizadas possam ser elencadas e executadas, com o devido registro.
- XLVIII.** A solução deve permitir que seja facultado aos gestores a subdelegação, temporária ou definitiva, dos privilégios de gestão a uma outra identidade, conforme as regras do negócio.
- XLIX.** A solução deve permitir, a qualquer tempo, que os gestores façam bloqueio parcial ou total dos privilégios das identidades geridas.
- L.** A solução deve permitir que sejam configurados os atributos livremente alteráveis pela identidade titular, os que desencadeiam notificação ao gestor e aqueles que não são alteráveis, exceto pelos administradores.
- LI.** As alterações efetuadas nas políticas de acesso devem ser replicadas automaticamente por todos os sistemas integrados, usuários e grupos.
- LII.** A solução deve possibilitar a utilização de rotinas externas para validação de informações.
- LIII.** A solução deve permitir que a exclusão lógica das identidades não implique a sua exclusão física nos sistemas integrados, pois muitos deles mantêm registro das transações por elas realizadas, que devem ser revinculadas no caso de recriação das mesmas.



- LIV.** A solução deve possuir interface Java ou Webservices que forneça benefícios como integração com aplicações para ações de inserção, exclusão, atualização, e ações em massa na base de usuários da solução.
- LV.** A solução deve fornecer comunicação segura entre todos os componentes que a compõem, garantindo a confidencialidade e integridade dos dados.
- LVI.** A solução deve possibilitar nativamente ou através de customizações nativas (funcionalidade nativa customizada) o envio de alertas de erros em transações, através de algum tipo de mecanismo de comunicação, como: *traps* SNMP, e-mail ou SMS.
- LVII.** A solução a ser contratada deverá atender aos seguintes requisitos de gestão de senhas:
- a)** A solução deve permitir a criação de políticas de senhas, incluindo requisitos de formação, periodicidade de troca e bloqueio por limite de erros, observadas as limitações dos sistemas integrados.
 - b)** Em qualquer interface da solução, os campos destinados ao preenchimento de senhas devem ser mascarados, com caracteres apropriados.
 - c)** A solução deve permitir e controlar o estabelecimento de senha inicial e descartável para as identidades criadas, nos diversos sistemas integrados.
 - d)** A solução deve permitir a criação de políticas de recuperação ou renovação de senhas por parte dos administradores, independentemente para cada sistema integrado.
 - e)** A solução deve permitir que cada identidade cadastre os atributos relativos à recuperação e renovação de senha, como perguntas e respostas, e esse conteúdo deve ficar armazenado criptografado.
 - f)** A solução deve permitir, através de ferramenta própria ou página web, em qualquer etapa de acesso aos sistemas integrados e de uso das estações de trabalho com o sistema operacional ativo, com ou sem autenticação efetuada, que uma identidade recupere ou renove sua senha, através de desafios previamente cadastrados, de acordo com as políticas de senhas estabelecidas, sem intervenção de terceiros.
 - g)** A solução deve permitir que a senha de usuário seja replicada de forma automática para um ou vários sistemas integrados, respeitando as limitações de cada um desses sistemas.
 - h)** A solução deve permitir que a senha, após recuperada ou renovada no recurso de autorrecuperação, seja replicada para todos os sistemas provisionados.
 - i)** A recuperação ou renovação de senha feita por usuários (seja via Web ou via recurso Ctrl+Alt+Del do MS Windows) deve ser replicada automaticamente para o(s) sistema(s) a que se destina. Caso seja necessário instalar software nessas estações, o fornecedor vencedor efetuara essa implementação sem nenhum ônus adicional para a SEF/MG e em conformidade com as diretrizes da política de segurança desta Secretaria..
- LVIII.** A solução a ser contratada deverá atender aos seguintes requisitos de gestão de *workflows*:
- a)** A solução deve permitir a elaboração de fluxos de provisionamento ou *workflows*, incluindo etapas e ações de:
 - a.1)** solicitação de recursos ou perfis por usuários;
 - a.2)** detecção da criação de identidade ou alteração de atributos nos sistemas integrados;
 - a.3)** notificação dos gestores ou administradores sobre os eventos estipulados;



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

- a.4) espera por aprovação das solicitações feitas pelos gestores ou delegados;
 - a.5) alteração de atributos das entidades e demais atualizações, se necessário.
- b) Os *workflows* devem permitir, entre outras funcionalidades:
- b.1) provisionamento de recursos para usuários;
 - b.2) execução de tarefas manuais ou automáticas, relacionadas aos sistemas não integrados;
 - b.3) tarefas de recursos;
 - b.4) alteração de atributos;
 - b.5) associação a grupos.
- c) A solução não deve impor restrições nos workflows em relação à:
- c.1) quantidade de aprovadores ou de etapas;
 - c.2) quantidade de registros feitos ou notificações enviadas;
 - c.3) quantidade de consultas feitas aos sistemas integrados para determinação do prosseguimento do fluxo.
- d) A solução deve permitir o andamento das solicitações de aprovação no caso de recursos com mais de um aprovador.
- e) O prosseguimento ou roteamento de cada *workflow* deve acontecer de forma automática, sem intervenção humana.
- f) A solução deve permitir o cadastro de aprovadores alternativos para os workflows pelos gestores.
- g) A solução deve permitir que escalonamentos sejam configurados para os workflows, de forma que solicitações não atendidas no tempo especificado sejam encaminhadas para uma rota alternativa.
- h) A solução deve permitir ao usuário solicitante, bem como aos administradores, o acompanhamento do estado atual do fluxo da solicitação.
- i) A solução deve permitir intervenção dos administradores no andamento de qualquer workflow.
- j) A solução deve permitir workflows distintos e aplicá-los adequadamente de acordo com os mais diversos parâmetros, incluindo, mas não restrito a:
- j.1) valores de atributos das identidades dos solicitantes;
 - j.2) tipo de recurso ou de perfil solicitado;
 - j.3) evento ou sistema originadores do workflow.
- k) Deve ser possível configurar suspensões ou permissões temporárias de certos privilégios, nos casos em que o tempo de aprovação passar do tempo especificado.



- l) Os *workflows* devem suportar integração com Webservices.
- m) Os *workflows* devem suportar a funcionalidade de cancelar a solicitação e informar o solicitante caso um prazo limite determinado pelo negócio expire.

LIX. A solução a ser contratada deverá atender aos seguintes requisitos de controle de acesso de forma nativa ou através de customizações nativas (funcionalidade nativa customizada):

- a) A solução deve suportar administração de usuários em listas de controle de acesso no MS Windows e UNIX.
- b) A solução deve possuir um servidor de diretório padrão LDAP nativo para armazenamento e controle de usuários e grupos.
- c) A solução deve ser capaz de operar com autenticação baseada em certificados digitais padrão X.509, não importando o meio – *tokens*, *smartcards*, entre outros.
 - c.1) A solução deve ser compatível com o padrão ICP-Brasil, suportando certificados do tipo A3 e A1, podendo, a critério da Comissão de Licitação, ser exigida dos licitantes a realização de uma Prova de Conceito para verificar o funcionamento da solução com um certificado ICP-Brasil.
- d) A solução deve suportar modelo híbrido de acesso, permitindo que acessos sejam atribuídos por associação a perfis ou por associação direta aos recursos requisitados.
- e) A solução deve permitir a gerência de privilégios de acesso dos usuários por meio de grupos.
- f) Deve ser possível para o gestor de um recurso e para os administradores visualizar, de forma consolidada, os usuários e grupos que lhe têm acesso.
- g) A solução deve permitir o controle granular do acesso a sistemas e a recursos aos quais está integrada, ou seja, o gestor pode solicitar adição ou retirada de um acesso que não esteja contemplado no(s) perfil(is) para ele disponibilizados.
- h) A solução deve disponibilizar mecanismos que permitam a integração da solução de controle de acesso com aplicações em todos os ambientes de desenvolvimento e aplicação.
- i) A solução deve listar apenas os recursos e perfis cabíveis e geridos para a área de cada gestor.
- j) A solução deve ter mecanismo nativo que bloqueie ou exclua acessos, a partir de regras estabelecidas.
 - j.1) As regras devem poder ser criadas independentemente para cada sistema integrado.
 - j.2) As regras devem levar em conta critérios como janelas de horário, perfis e endereço de origem da requisição de acesso.

LX. A solução a ser contratada deverá atender aos seguintes requisitos de gestão de perfis:

- a) A solução deve garantir que alterações feitas em um perfil sejam automática e imediatamente replicadas às identidades associadas ao perfil.
- b) A solução deve prover perfis e privilégios às identidades de acordo com atributos como, por exemplo, cargo, função e centro de custo.
- c) A solução deve permitir a criação de perfis administrativos diferenciados na interface administrativa do sistema.



- d) A solução deve permitir a inserção de informações descritivas sobre os perfis criados, em campos e quantidades configuráveis.

LXI. A solução a ser contratada deverá atender aos seguintes requisitos de gestão de formulários:

- a) A solução deve suportar a criação e manutenção, em interface gráfica nativa, sem necessidade de programação ou codificação, de formulários com os seguintes propósitos, entre outros:

a.1) preenchimento de dados cadastrais de uma identidade;

a.2) preenchimento de perguntas e respostas para recuperação ou renovação de senhas;

a.3) preenchimento de requisição de adição, alteração e remoção de acessos de uma identidade.

- b) Nos formulários de requisição de acesso para usuários, a solução deve ser capaz de facultar ao gestor de área a omissão de determinados recursos (Ex: limitar algumas permissões na tela)..

- c) A solução deve permitir o preenchimento automático de valores do formulário, quando cabível, e permitir ou bloquear alterações conforme inciso LI do subitem 1.2.1 deste Termo de Referência.

LXII. A solução a ser contratada deverá atender aos seguintes requisitos de registro e auditoria:

- a) A solução deve registrar todas as atividades realizadas por usuários, gestores, administradores e workflows, e manter histórico dessas atividades.

- b) A solução deve prover instrumento que gere relatórios pré-formatados e configuráveis, sem necessidade de codificação, para que gestores e administradores validem os acessos e perfis de usuários.

- c) A solução deve oferecer, nativamente ou através de customizações, os seguintes relatórios:

c.1) todos os grupos, recursos ou perfis de um usuário;

c.2) todos os usuários de um grupo, perfil ou recurso;

c.3) histórico de manutenção de perfis de identidades;

c.4) lista de usuários por categoria, atributos ou direitos associados;

c.5) histórico de usuários provisionados para determinado recurso ou perfil.

- d) A solução deve prover dados estatísticos sobre volume de solicitações gerenciadas pelos workflows, como solicitações pendentes, solicitações aprovadas, solicitações recusadas etc.

- e) A solução deve permitir, de forma nativa e embutida, a impressão legível e formatada em formato A4 ou carta dos relatórios e listagens providos e deve permitir a exportação em diversos formatos, como PDF, CSV, HTML, entre outros.

LXIII. A solução deve implementar o padrão SSO (Single Sign-On) para Web evitando que o usuário seja obrigado a guardar mais de um *login* e senha ou ter de autenticar-se novamente em outras aplicações.

LXIV. A solução deve redirecionar um usuário automaticamente para a tela de *logon* caso ele tente acessar um recurso protegido de uma aplicação sem estar autenticado.



- LXV.** A solução deve permitir a publicação e gestão de avisos para os usuários de forma passível de customização, tais como aviso de aplicação indisponível devido a uma manutenção programada..
- LXVI.** A solução deve permitir a publicação e gestão de perguntas frequentes – FAQ de forma passível de customização, a serem disponibilizadas para os usuários, tais como dúvidas sobre como proceder em caso de esquecimento da senha e similares..
- LXVII.** A solução deve possibilitar que o perfil do usuário seja recuperado nas aplicações/sistemas para a criação de filtros de dados (permissões nas aplicações) via JAAS, Serviços de Autenticação e APIs Java.
- LXVIII.** A solução deve possibilitar a utilização do sistema de segurança em diferentes plataformas (Windows, Linux, UNIX, Mainframe) e fazer o controle de acesso de aplicações instaladas em diferentes servidores de aplicação (Apache, IIS, Tomcat, JBoss ou outro servidor JEE)..
- LXIX.** A solução deve possuir uma API Java ou de serviços (*Web Services*) com funções utilitárias (troca de senha, lembrar senha por código de reativação, buscar dados do usuário, buscar dados de credenciais etc.)
- LXX.** A solução deve prover agentes de controle de acesso de forma nativa para aplicações na plataforma Java.
- LXXI.** A solução deve permitir a gestão do acesso à aplicação em vários ambientes (desenvolvimento, homologação e produção), com diferentes níveis de acesso (os perfis do usuário são independentes em cada ambiente).
- LXXII.** A solução deve permitir a exportação e importação dos dados de gestão de segurança da aplicação entre os ambientes de desenvolvimento, homologação e produção.
- LXXIII.** A solução deve possuir funcionalidades para gestão do cadastro dos usuários (incluir, alterar, excluir e consultar dados de usuários), mantendo pelo menos os seguintes atributos:
- a) Identificador único do usuário (*login*);
 - b) Dados pessoais (nome completo, *e-mail* e ramal);
 - c) Pergunta de desafio;
 - d) Unidade Administrativa à qual está vinculado ou outra restrição personalizada;
- LXXIV.** A solução deve permitir que seja criada, a partir do cadastro de usuários, uma senha aleatória, que será gerada pelo próprio sistema e enviada para o *e-mail* informado
- LXXV.** A solução deve verificar a força das senhas que serão criadas pelos usuários, atestando se possuem um mínimo de complexidade, conforme política de senhas a ser definida pela SEF/MG.
- LXXVI.** A solução deve possuir funcionalidade que permita a cada usuário alterar sua própria senha e atualizar seus dados pessoais, sem necessidade de intervenção do gestor de segurança.
- LXXVII.** A solução deve possuir funcionalidade para tratamento de situações de esquecimento de senhas por usuários, através da geração de um código de reativação (com prazo de expiração) e pergunta de desafio.
- LXXVIII.** A solução deve possuir funcionalidade que realize o bloqueio da conta de um usuário após N tentativas de *login* com insucesso, sendo N configurado de acordo com a política de senhas definida pela SEF/MG.
- LXXIX.** A solução deve possuir funcionalidade que não permita que o usuário utilize as últimas N senhas já utilizadas anteriormente, sendo N configurado de acordo com a política de senhas definida pela SEF/MG.



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

- LXXX.** A solução deve possuir funcionalidade que faça a expiração da senha após um período de N dias sem acesso, sendo N configurado de acordo com a política de senhas definida pela SEF/MG.
- LXXXI.** A solução deve impedir o *logon* simultâneo em máquinas diferentes.
- LXXXII.** A solução deve garantir que um usuário com permissão de gestão de segurança só conceda permissões a outros usuários a partir das permissões que tenha possibilidade de conceder.
- LXXXIII.** A solução deve permitir a hierarquia entre grupos de gestão de usuário (gestores do portal), de forma que um determinado grupo só possa gerar usuários de grupos inferiores (Root, Administrador, Gestor, Criador, Padrão). Ou seja, permitir diferentes privilégios para os usuários na Gestão de Segurança, da seguinte forma:
- a)** Root: Acesso a todas as funcionalidades da gestão de segurança.
 - b)** Administrador: Acesso a todas as funcionalidades de gestão das aplicações e usuários sob sua responsabilidade, de acordo com as restrições existentes.
 - c)** Criador de usuários: Acesso às funcionalidades de criação de usuários.
 - d)** Padrão: Acesso às aplicações autorizadas.
- LXXXIV.** A solução deve permitir a gestão da segurança de mais de uma aplicação/sistema, realizando toda a gestão dos grupos das aplicações em separado.
- LXXXV.** A solução deve permitir a implementação de restrição nos níveis de menu, submenu, subsubmenu, página, campos de uma página e botões da página.
- LXXXVI.** Possuir funcionalidade que permita a configuração de domínios de acesso (restrições), de modo que privilégios de acesso sejam concedidos por domínio (restrição), entendendo-se como domínio qualquer atributo definido pelo gestor de segurança que será vinculado ao usuário, tais como Unidade Administrativa, Regional etc. Deve ser possível, com esse recurso, conceder permissão a um usuário para realizar ações específicas em domínios autorizados, ficando este impossibilitado de realizar a mesma ação em outras Unidades Administrativas, Regionais etc.
- LXXXVII.** Possibilitar consulta à lista de usuários e perfis por domínio (restrição) e por aplicação/sistema.
- LXXXVIII.** Possibilitar a geração de relatórios de forma agendada ou gerados instantaneamente.
- LXXXIX.** Possibilitar que as permissões para geração e visualização dos relatórios sejam determinadas através dos grupos (perfis) ou usuários do sistema de segurança.
- XC.** Suportar os requisitos contidos nas alíneas de “a” a “cn” abaixo, que estão baseados no Manual de Desenvolvimento e Aquisição de Sistemas Seguros (MDASS) - volume 1 do governo de Minas Gerais, disponível em: <http://www.egov.mg.gov.br/download?arquivo=2023> , estando consignados apenas os requisitos aplicáveis à solução contratada e que dependem de recursos providos por ela, tendo em vista seu perfil de segurança e das principais aplicações que serão a ela integradas.

Alínea	Classe	Família	Descrição	Mecanismos necessários para implementação
a	FAU – Auditoria de Segurança	Resposta Automática de Auditoria	Todos os eventos que possam indicar violação de segurança deverão ser registrados.	- Manipulação indevida de campos; (APLICAÇÃO) - Manipulação de parâmetros na URL; (APLICAÇÃO) - Tentativa de acesso por força bruta (usuários distintos); - Tentativa de recuperação



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

				de senha; - Violação de acesso; IMPORTANTE: Podem existir outros tipo de eventos de acordo com a especificação da aplicação.
b		Geração de Dados de Auditoria	A utilização bem sucedida das funções administrativas da solução de gestão de identidade e acesso deverá ser registrada.	Registro histórico das alterações de configurações dos sistemas. As configurações são parâmetros alterados na própria aplicação que podem interferir no seu funcionamento.
c		Geração de Dados de Auditoria	Todas as tentativas de acesso às funções administrativas deverão ser registradas. A utilização bem-sucedida de funções privilegiadas deverá ser registrada.	Todos os acessos às funções administrativas da aplicação deverão estar associados apenas aos perfis com autorização. Todas as alterações nas funções administrativas deverão ser registradas em um log de auditoria.
d		Geração de Dados de Auditoria	Cada ação registrada deverá ter a devida identificação do autor.	Toda ação registrada deverá ter a devida identificação do autor.
e		Geração de Dados de Auditoria	Todas as atividades deverão ser registradas, excetuando-se os valores de senhas. As marcas de tempo devem ter uma referência oficial bem definida e confiável.	Todas as atividades deverão ser registradas, excetuando-se os valores de senhas. As marcas de tempo devem ter uma referência oficial bem definida e confiável. Os registros de log deverão possuir registro de data e hora sincronizados com o Observatório Nacional.
f		Análise de Auditoria de Segurança	Deverão ser estabelecidos padrões de uso do sistema para cada grupo de usuários e, caso haja incoerência ou desvio, deverá	Todo usuário deverá estar associado a um perfil de acesso. E todo perfil de acesso poderá possuir um padrão de acesso baseado em horário, duração e frequência. Caso haja incoerência ou desvio, deverá ser realizado um registro.



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			ser realizado registro. (Ex: poderá possuir um padrão de acesso baseado em horário, duração e frequência)	
g		Revisão da Auditoria de Segurança	Somente usuários explicitamente autorizados poderão acessar os registros de auditoria.	Criação obrigatória de perfil específico para auditoria. Este perfil terá o acesso à todos os registros de auditoria. Será de responsabilidade do gestor definir quem será o auditor.
h		Revisão da Auditoria de Segurança	As funções de leitura e remoção de registros de auditoria deverão ser segregadas para usuários distintos.	A leitura poderá ser feita por perfis autorizados. A remoção de registros de auditoria não poderá ser realizada por nenhum perfil.
i		Revisão da Auditoria de Segurança	Deverão ser categorizados os tipos de registros de auditoria para que sejam designados tipos de usuários com permissão específica para seu acesso.	Definir perfis com permissão de visualização de logs de forma segregada. Exemplo: o perfil de auditor de processo pode visualizar logs de processos, enquanto o perfil de auditor de segurança pode visualizar logs de segurança.
j		Seleção de Eventos de Auditoria de Segurança	Deverão ser incorporadas ferramentas de forma nativa ou nativa customizada de seleção para facilitar a visualização dos registros de auditoria, como, por exemplo, a classificação dos eventos por ID, usuário, data/hora etc.	Deverá haver funções para criar relatórios e poder inserir os campos de registros de auditoria desejados, com as opções para classificação por campo de ID, usuário, data/hora, tipo de evento, IP etc., podendo ser realizadas classificações dos registros pelos campos pesquisados.
k		Armazenamento dos Eventos de Auditoria de Segurança	Os registros de auditoria não poderão ser removidos por	Utilização de sistema de controle de acesso do sistema operacional.



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			usuários, mesmo os com direitos administrativos.	
l	FCO - Comunicação	Irretratabilidade da origem	O sistema deverá apresentar ao usuário garantias de que é, efetivamente, o sistema acessado.	Definir mecanismos, tais como certificado digital de servidor (SSL) e informativos para deixar claro para o usuário que a aplicação é realmente o sistema que ele pretende acessar.
m		Irretratabilidade da Origem	Cada resposta enviada aos usuários ou armazenada pelo sistema deverá conter registro de tempo.	Utilizar certificado digital de servidor (SSL) para garantir a origem. Armazenar em logs informações sobre tempo (data e hora) das transações (requisição e resposta).
n		Irretratabilidade do Destinatário	Cada usuário deverá ter identificação individual	Elaborar regra para garantir o <i>login</i> único por usuário na aplicação. Ex.: - Está vinculado a um campo identificador único, como: Matrícula, CPF, RG ou outros; - Poderá ser aplicável o uso de Certificação Digital ICP-Brasil, recursos biométricos ou cifra de uso único (<i>One Time Pad</i> - OTP).
o		Irretratabilidade do Destinatário	As credenciais de acesso ao sistema não podem ser compartilhadas por meios técnicos	- Não permitir <i>logins</i> simultâneos em máquinas diferentes.
p		Irretratabilidade do destinatário	Deverá ser realizado acesso utilizando, no mínimo, duplo fator de autenticação.	Para certas funções críticas do sistema, deverão ser exigidos múltiplos mecanismos de autenticação, tais como: - Acesso por certificado digital em hardware criptográfico, como <i>tokens</i> e <i>smartcards</i> - Recursos biométricos (impressão digital, registro vascular da mão, retina, etc.) - Cifra de uso único (<i>One Time Pad</i> - OTP) - Requisição de algum tipo de informação cadastral para confirmação e autenticação.



q	FDP – Proteção de Dados do Usuário	Operação Criptográfica	Operações criptográficas devem ser transparentes em tráfego por firewalls e NAT.	O tráfego criptografado de aplicações desenvolvidas/mantidas pela SEF/MG (ou por empresas por ela contratadas) não deve ser bloqueado em Firewall e/ou NAT. Ex: O uso de SSL ou criptografia na camada de aplicação (TCP) independe de firewalls e NAT
r		Operação Criptográfica	Deverão ser empregados algoritmos criptográficos públicos e tamanhos de chaves reconhecidamente seguros.	Empregar algoritmos criptográficos públicos e tamanhos de chaves reconhecidamente seguros. Ex: - Algoritmos criptográficos simétricos: AES, 3DES etc. e tamanhos de chaves recomendados pelo mercado. - Algoritmos criptográficos assimétricos: RSA, DSA etc. e tamanhos de chaves recomendados pelo mercado.
s		Operação Criptográfica	As operações que envolvam o uso de chaves criptográficas deverão ser documentadas de forma detalhada.	Criação de procedimentos para uso e controle de operações que envolvam chaves criptográficas.
t		Política de Controle de Acesso	Deverá ser estabelecida uma matriz documentando as permissões concedidas aos usuários por tipo de usuário e por tipo de informação disponibilizada pelo sistema (matriz de permissões).	Todos os perfis de acesso e suas funcionalidades deverão ser documentados (matriz documentando as permissões concedidas aos usuários por tipo de usuário e por tipo de informação disponibilizada pelo sistema – matriz de permissões).
u		Funções de Controle de Acesso	Com base na matriz de permissões, devem ser estabelecidos acessos sob o princípio do menor privilégio. Também deverão ser	Com base na matriz de permissões, devem ser estabelecidos acessos sob o princípio do menor privilégio (um usuário é criado sem nenhuma permissão, por padrão). Também deverão ser estabelecidos critérios de separação de funções, com regras baseadas na necessidade de acesso dos



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			<p>estabelecidos critérios de separação de funções, com regras baseadas na necessidade de acesso dos grupos de usuários e objetivos no sistema. Deverão ser agrupados os usuários com base nas funções de suporte ao sistema: gerenciamento do sistema, gerenciamento de configurações, programação, testes/validação de qualidade, segurança. Os grupos de administração, auditoria e segurança não podem ser acumulados.</p>	<p>grupos de usuários e objetivos no sistema. Deverão ser agrupados os usuários com base nas funções de suporte ao sistema: gerenciamento do sistema, gerenciamento de configurações, programação, testes/validação de qualidade, segurança. Os grupos de administração, auditoria e segurança não podem ser acumulados.</p>
V		Funções de Controle de Acesso	<p>Deverão ser definidas funcionalidades de controle de acesso, como:</p> <ul style="list-style-type: none">- Listas de Controle de Acesso (ACLs);- Especificações de controle de acesso com base de tempo;- Especificações de controle de acesso com base na origem;- Atributos de controle de acesso do proprietário.	<p>Definir funcionalidades de controle de acesso, como:</p> <ul style="list-style-type: none">- Listas de Controle de Acesso (ACLs) na forma de perfis de segurança detalhados;- Especificações de controle de acesso com base de tempo (datas, dias da semana, horários do dia, frequência e duração);- Especificações de controle de acesso com base na origem (políticas de acesso e autorização diferentes para cada módulo);- Atributos de controle de acesso do proprietário (aplicável a arquivos, banco de dados, recursos do sistema operacional, processos etc.).



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

w		Funções de Controle de Acesso	Atributos de identificação deverão ser estabelecidos para usuários, objetos, e demais elementos de sistema que terão algum tipo de acesso, assim como seus grupos. Também deverão ser especificados os atributos de segurança requeridos para cada tipo de acesso.	Permitir a identificação e gestão dos atributos de identificação para usuários, objetos, e demais elementos de sistema que terão algum tipo de acesso, assim como seus grupos. Também deverão ser especificados os atributos de segurança requeridos para cada tipo de acesso.
x		Funções de Controle de Acesso	Complementarmente, devem ser estabelecidas listas que explicitem os acessos que serão negados, permitidos e os casos de exceção (Ex: permitir criar uma regra de negação de acesso a um recurso).	Permitir a definição de listas que explicitem os acessos que serão negados e casos de exceção além das permissões já concedidas.
y		Autenticação de Dados	Deverão ser estabelecidos controles para a autenticação de dados, sendo criadas trilhas de auditoria.	Implementar trilhas de auditoria de dados da aplicação, registrando alterações de estados ou representação dos dados da aplicação.
z		Autenticação de Dados	Deverá haver controles que evidenciem a autenticidade dos dados críticos, de forma técnica ou operacional.	Utilizar algoritmos de resumo (<i>hash</i>) (Ex: SHA1)/códigos de autenticação de mensagens (MAC) para garantir a autenticidade e integridade de informações sensíveis ou críticas, armazenadas ou transmitidas.
aa		Exportação de Dados	Por padrão, dados utilizados pelo sistema que sejam	Para o caso de exportação nativa da aplicação (ex: PDF, XLS etc.), considerar o que foi especificado nos requisitos de sistema em



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			classificados como sensíveis ou confidenciais deverão ser explicitamente preservados ou simplesmente ignorados em processos de exportação, devendo permitir a customização nativa (funcionalidade nativa customizada) dos atributos exportados em relatórios de acordo com a classificação da informação.	termos de classificação de informação. Considerar que os dados de banco de dados e sistemas de arquivo são sigilosos, a menos que haja disposição explícita em contrário. Tratar por exceção.
ab		Exportação de Dados	Deverá ser definido um fluxo de exportação de dados. Caso os dados sejam sensíveis ou confidenciais, deverão ser estabelecidos controles lógicos (como criptografia) ou físicos para restringir o acesso aos dados. Obrigatoriamente, os dados sensíveis ou confidenciais deverão estar acompanhados dos dados de usuário/sistema, de forma integral, ou por referência direta. Os meios de exportação deverão utilizar controles que impeçam o vazamento de	Definir um fluxo de exportação de dados. Caso sejam sensíveis ou confidenciais, deverão ser estabelecidos controles lógicos (como criptografia) ou físicos para restringir o acesso aos dados. Obrigatoriamente, os dados sensíveis ou confidenciais deverão estar acompanhados dos dados de usuário/sistema, de forma integral, ou por referência direta. Os meios de exportação deverão utilizar controles que impeçam o vazamento de informações.



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			informações. A solução deverá permitir a customização nativa (funcionalidade nativa customizada) dos atributos exportados em relatórios de acordo com a classificação da informação.	
ac		Política do Fluxo de Informação	Deverá ser criada uma política que descreva os fluxos da informação, declarando suas origens, caminhos e destinos.	Criar uma política que descreva os fluxos da informação, declarando suas origens, caminhos e destinos.
ad		Política do Fluxo de Informação	Deverão ser especificadas listas de sujeitos (usuários, computadores, processos), informações (e-mail, documentos) e operações que serão incluídos no fluxo de informação. Esse fluxo deverá fazer parte de uma política, onde são definidos os requisitos de segurança para cada componente listado.	Criar listas de sujeitos (usuários, computadores, processos), informações (e-mail, documentos) e operações que serão incluídos no fluxo de informação. Esse fluxo deverá fazer parte de uma política, onde são definidos os requisitos de segurança para cada componente listado.
ae		Funções do Fluxo de Informação	Deverão ser empregados controles para assegurar que seja mantida a privacidade das informações em trânsito.	Obrigatório o uso de criptografia, dependendo do requisito. Exemplos: - HTTPS (SSL/TLS) - 3DES, AES etc.



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

af		Funções do Fluxo de Informação	Deverá haver monitoramento e, quando possível, bloqueio de canais dissimulados ou de comunicações ilícitas a partir do sistema e para o sistema.	Utilização de solução de firewall e IDS/IPS nas redes onde os sistemas estão instalados. Adicionalmente, utilizar solução de DLP (<i>Data loss prevention</i>). Essas ferramentas não integram a solução de gestão de identidade a ser ofertada. A solução de gerência de identidade ofertada deverá ser capaz de ser utilizada em conjunto com essas ferramentas de segurança e de ser protegida por elas.
ag		Importação de Dados	A importação de dados sem atributos de segurança deverá ocorrer de forma estruturada, observando seu formato.	Conforme regra de negócio, a importação de dados sem atributos de segurança deverá ocorrer de forma estruturada, observando seu formato.
ah		Importação de Dados	Dados com atributos de segurança, ao serem importados para o sistema, deverão ser verificados quanto ao seu formato e consistência.	Conforme requisito de negócio, dados com atributos de segurança, ao serem importados para o sistema, deverão ser verificados quanto ao seu formato e consistência (validação).
ai		Proteção da Informação Residual	Deverão ser listados os tipos de informação passíveis de exclusão.	Especificação de regras de negócio que descrevam os tipos de dados que poderão ser excluídos do sistema.
aj		Proteção da Informação Residual	Dados excluídos não poderão ser acessíveis, diretamente, por usuários ou administradores. Dados temporários armazenados em memória compartilhada ou em arquivos deverão ser sobrescritos ou removidos de forma segura.	Implementação da exclusão física para os casos em que for necessário, impedindo que administradores de infraestrutura possam realizar o <i>undelete</i> de um arquivo ou registro.



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

ak		Reversão	Alterações no sistema deverão ser precedidas de mecanismos de <i>backup</i> para que seja possível reverter para o último ponto reconhecidamente funcional.	Adotar mecanismos de <i>backup</i> dos arquivos da aplicação e de suas configurações, incluindo instalação e configurações do <i>software</i> básico, antes das atualizações de versão da aplicação e do ambiente operacional.
al		Reversão	Todas as funções do sistema deverão ter condições de ser revertidas para a última configuração válida.	Criar mecanismos que permitam ao usuário restaurar a última configuração válida, através dos arquivos de <i>backup</i> .
am		Integridade de Dados Armazenados	Devem ser estabelecidos controles automatizados para a recuperação de dados indevidamente alterados.	Para os casos que necessitem dessa funcionalidade, conforme especificação, criar mecanismos para retornar/recuperar informações alteradas indevidamente.
an		Confidencialidade dos Dados em Trânsito dos Usuários	Dados de usuários deverão ser mantidos sob sistema de controle contra acesso indevido e vazamento.	Utilizar mecanismo de controle de identidade e acesso, que pode ser provido por uma ferramenta.
ao		Confidencialidade e dos Dados em Trânsito dos Usuários	Os dados de usuários deverão ser protegidos de modo que, mesmo em caso de falha dos controles dos canais, não sejam expostos.	Conforme requisito de negócio, os dados deverão ser criptografados pela aplicação, independentemente do canal.
ap	FIA – Identificação e Autenticação	Falhas de Autenticação	Deve ser possível configurar ou customizar de forma nativa (funcionalidade nativa customizada) a seguinte regra:	Após a segunda falha de autenticação com a mesma credencial, o usuário deverá ser encaminhado para sistema de recuperação de credenciais.



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			após a segunda falha de autenticação com a mesma credencial, o usuário deverá ser encaminhado para sistema de recuperação de credenciais.	
aq		Falhas de Autenticação	Deve ser possível configurar ou customizar de forma nativa (funcionalidade nativa customizada) a seguinte regra: após a terceira tentativa de autenticação sem sucesso, com uma mesma credencial, o usuário deverá ter seu acesso bloqueado por 15 minutos, ou conforme a política local.	Após a terceira tentativa de autenticação sem sucesso, com uma mesma credencial, o usuário deverá ter seu acesso bloqueado por 15 minutos, ou conforme a política local.
ar		Falhas de Autenticação	Deve ser possível configurar ou customizar de forma nativa (funcionalidade nativa customizada) a seguinte regra: após a quinta tentativa de acesso sem sucesso, independente da credencial utilizada, o acesso do usuário ao sistema deverá ser bloqueado por 15 minutos para o sistema ou computador de origem.	Após a quinta tentativa de acesso sem sucesso, independente da credencial utilizada, o acesso ao sistema deverá ser bloqueado por 15 minutos para o sistema/ computador de origem.
as		Falhas de Autenticação	O desbloqueio de credenciais	O desbloqueio de credenciais poderá ser



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			poderá ser realizado somente mediante procedimento administrativo formal.	realizado somente mediante procedimento administrativo formal.
at		Definição de Atributos de Usuários	Os atributos de segurança de um usuário deverão ser relacionados diretamente a esse. Dessa forma, espera-se que uma alteração em um usuário não gere impactos em outros.	Todo usuário deverá está associado a um perfil de acesso. Além disso, é necessário ter uma funcionalidade para atribuir funções individualmente. Isso significa, por exemplo, que as chaves de um usuário são exclusivas.
au		Especificação de Segredos	O usuário poderá definir segredos que serão utilizados para autenticação no sistema. Esses segredos devem ter complexidade mínima e prazo de validade definida por política, devidamente verificados pelo sistema.	O usuário poderá definir segredos que serão utilizados para autenticação no sistema. Esses segredos devem ter complexidade mínima e prazo de validade definida por política, devidamente verificados pelo sistema. Adicionalmente, deve ser definida política de senhas. Diretrizes para implementação da política de senhas: Convém que todos os usuários sejam informados de que devem, obrigatoriamente: a) manter a confidencialidade das senhas;b) evitar manter anotadas senhas (por exemplo, em papel, arquivos ou dispositivos móveis), a menos que elas possam ser armazenadas de forma segura e o método de armazenamento esteja aprovado; c) a senha deverá ser alterada sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;d) selecionar senhas de qualidade, com um tamanho mínimo, que sejam:1) fáceis de lembrar; 2) não baseadas em nada que alguém facilmente possa adivinhar ou obter usando informaçõesrelativas



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

				<p>à pessoa, por exemplo, nomes, números de telefone e datas de aniversário; 3) não vulneráveis a ataque de dicionário (por exemplo, não consistir em palavras inclusas no dicionário); 4) isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos; e) modificar senhas regularmente ou com base no número de acessos (convém que senhas de acesso a contas privilegiadas sejam modificadas mais frequentemente que senhas normais) e evitar a reutilização do ciclo de senhas antigas;f) modificar senhas temporárias no primeiro acesso ao sistema;g) não incluir senhas em nenhum processo automático de acesso ao sistema, por exemplo, armazenadas em uma macro ou em funções-chave; h) não compartilhar senhas de usuários individuais; i) não utilizar a mesma senha com finalidades profissionais e pessoais.</p>
av		Especificação de Segredos	A geração de segredos também poderá ser realizada pelo sistema, de forma aleatória, obedecendo minimamente aos critérios definidos por política.	A geração de senhas também poderá ser realizada pelo sistema, de forma aleatória, obedecendo minimamente aos critérios definidos por política.



aw		Autenticação de Usuários	<p>Todo segredo informado pelo usuário deverá ser oculto ou exibido de forma mascarada. Os segredos devem ser sempre armazenados/manipulados em forma criptografada ou em resumo (<i>hash</i>) com qualidade criptográfica. A verificação de uma credencial, para que seja concedido acesso a um recurso, deverá realizar as seguintes etapas, não necessariamente e nesta ordem:</p> <ol style="list-style-type: none">1. Se o modo de acesso utilizado para acessar o recurso é proibido, o acesso deverá ser negado;2. Se o modo de acesso utilizado para acessar o recurso é permitido, o acesso deverá ser concedido;3. Se o modo de acesso utilizado para acessar o recurso é proibido para todos os grupos dos quais o usuário é membro, o acesso deverá ser negado;4. Se o modo de acesso utilizado para	<ol style="list-style-type: none">1. Além do processo de autenticação de acesso de usuários, para determinadas aplicações onde existam transações críticas deverá ser realizado um processo de nova autenticação (conforme especificação).2. As telas de autenticação deverão utilizar obrigatoriamente protocolo seguro.3. Os segredos devem ser exibidos com caracteres especiais.4. Os segredos devem ser armazenados em formato de <i>hash</i> (SHA1) no banco de dados ou de forma criptografada.
----	--	--------------------------	---	---



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			<p>acessar o recurso é permitido para qualquer grupo do qual o usuário é membro, o acesso deverá ser concedido; 5. Se o modo de acesso utilizado para acessar o recurso é proibido ao público, o acesso deverá ser negado; 6. Se o modo de acesso utilizado para acessar o recurso é permitido, o acesso deverá ser concedido; 7. Qualquer outra tentativa de acesso deverá ser negada.</p>	
ax		Autenticação de Usuários	<p>Deve ser possível configurar ou customizar de forma nativa (funcionalidade nativa customizada) a seguinte regra: usuários anônimos não serão autorizados. A autenticação de usuários deverá ocorrer imediatamente após a apresentação de um aviso sobre o uso e as responsabilidades do usuário no sistema. Nenhuma outra função de consulta ou navegação</p>	<p>Usuários anônimos não serão autorizados para recursos protegidos. A autenticação de usuários deverá ocorrer imediatamente após a apresentação de um aviso sobre o uso e as responsabilidades do usuário no sistema. Nenhuma outra função de consulta ou navegação poderá ser realizada anteriormente à autenticação. Um mesmo usuário não poderá ter acesso concomitante ao sistema. Ao acessar, o mesmo será avisado sobre o número de acessos efetuados, data e hora do último acesso válido e a validade de suas credenciais. É importante que seja incluída uma mensagem na tela inicial do sistema, contendo informações similares às contidas no</p>



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			<p>poderá ser realizada anteriormente à autenticação. Um mesmo usuário não poderá ter acesso concomitante ao sistema. Ao acessar, o mesmo será avisado sobre o número de acessos efetuados, data e hora do último acesso válido e a validade de suas credenciais</p>	<p>seguinte exemplo: “Este sistema e todos os dados por ele tratados são propriedade da Secretaria de Estado de Fazenda de Minas Gerais e devem ser usados exclusivamente para tarefas autorizadas. Caso você não seja usuário autorizado, feche o sistema imediatamente. Usuários autorizados devem conhecer seus direitos no sistema e, mesmo se permitido pelo sistema, não devem acessar dados fora de seus direitos. Todas as ações no sistema são de responsabilidade do usuário autenticado (que efetuou <i>logon</i>) e são registradas em trilhas de auditoria”.</p>
ay		Autenticação de Usuários	<p>O uso de múltiplos fatores de autenticação (pelo menos duplo) será obrigatório para acessar o sistema e realizar operações de alterações em dados.</p>	<p>Conforme requisito de negócio, em casos específicos deve-se utilizar dois mecanismos de autenticação, tais como acesso por certificado digital e exigindo algum tipo de informação cadastral para confirmação e autenticação.</p>
az		Ligação usuário-assunto	<p>Por padrão, nenhum usuário poderá realizar uma ação em nome de outro.</p>	<p>Não deverão ser criados usuários genéricos ou permitir que o administrador assuma o perfil de outro usuário. As atividades de administração, gerenciamento de segurança e auditoria não devem ser acumuladas pelos mesmos usuários.</p>
ba		Ligação usuário-assunto	<p>Todas as ações realizadas pelos usuários serão vinculadas aos mesmos. As operações administrativas que envolvam a alteração de atributos de segurança dos usuários deverão ser</p>	<p>Todas as ações realizadas pelos usuários serão vinculadas aos mesmos. As operações administrativas que envolvam a alteração de atributos de segurança dos usuários deverão ser listadas e verificadas. Essas medidas evitam, por exemplo, que um administrador execute uma ação em nome de outro usuário. Todos os usuários deverão</p>



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			listadas e verificadas.	estar associados a um perfil de acesso que contenha as funções pré-definidas. - Todas as alterações em operações administrativas deveram ser registradas em logs de auditoria. - Convém que todos os usuários tenham um identificador único (ID de usuário) para uso pessoal e exclusivo, e convém que uma técnica adequada de autenticação seja escolhida para validar a identidade alegada por um usuário.
bb	FMT – Gerenciamento de Segurança	Gerenciamento de funções do sistema	Deverá haver uma matriz de funções de usuários, segregando atividades de administração, configuração de segurança e auditoria.	Criar uma matriz de funções de usuários, segregando atividades de administração, configuração de segurança e auditoria.
bc		Gerenciamento de funções do sistema	O sistema deverá permitir a criação de usuários de administração de segurança independentes, ou seja, que possuam funções distintas do administrador do sistema e que não possam receber interferência desse. Assim, por exemplo, novos usuários de administração de segurança poderão ser criados apenas pelo primeiro administrador de segurança.	O sistema deverá contar, nativamente, com usuários de administração de segurança independentes, ou seja, que possuam funções distintas do administrador do sistema e que não possam receber interferência desse. Assim, por exemplo, novos usuários de administração de segurança poderão ser criados apenas pelo primeiro administrador de segurança. Recomenda-se que os usuários nativos tenham direitos de criar novos usuários das mesmas categorias. Por exemplo, auditores só poderão ser criados a partir de auditores.
bd		Gerenciamento de atributos de segurança	Deverão ser listadas as funções que criam, alteram ou removem	Listar as funções, na tela ou por relatórios, que criam, alteram ou removem atributos de segurança de usuários e funções do



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			atributos de segurança de usuários e funções do sistema.	sistema.
be		Gerenciamento de dados das funções de segurança	Somente administradores de segurança poderão alterar dados das funções de segurança.	Criação obrigatória de perfil específico para administradores de segurança. Esse perfil terá acesso a todas as funções de segurança. Será de responsabilidade do gestor definir quem serão os administradores de segurança.
bf		Gerenciamento de dados das funções de segurança	Qualquer alteração sobre as propriedades de usuários com esse poder de administração deverá ser registrada de forma indelével.	Gerar registros de logs para qualquer alteração sobre as propriedades de usuários com esse poder de administração, os quais deverão ser registrados de forma indelével.
bg		Revogação	Deverá haver confirmação dos direitos do usuário a cada entrada (<i>login</i>) no sistema. Assim, por exemplo, um usuário que tenha privilégios revogados deverá perdê-los, minimamente, na próxima autenticação no sistema.	Deverá haver confirmação dos direitos do usuário a cada entrada (<i>login</i>) no sistema. Assim, por exemplo, um usuário que tenha privilégios revogados deverá perdê-los, minimamente, na próxima autenticação no sistema.
bh		Revogação	Deverá haver confirmação dos direitos do usuário a cada ação no sistema. Assim, por exemplo, um usuário que tenha privilégios revogados deverá perdê-los, minimamente, no próximo	Deverá haver confirmação dos direitos do usuário a cada ação no sistema. Assim, por exemplo, um usuário que tenha privilégios revogados deverá perdê-los, minimamente, no próximo acesso a qualquer função do sistema.



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			acesso a arquivo.	
bi		Revogação	Deverá haver confirmação dos direitos do usuário a cada 10 minutos. Assim, por exemplo, um usuário que tenha privilégios revogados deverá perdê-los, no máximo, em 10 minutos.	Conforme especificação de negócio, deverá haver confirmação dos direitos do usuário em, no máximo, 10 minutos. Assim, por exemplo, um usuário que tenha privilégios revogados deverá perdê-los, no máximo, em 10 minutos.
bj		Validade dos atributos de segurança	Atributos de segurança deverão ter limitação de uso por tempo, de acordo com a política institucional. Dentre os atributos de segurança com validade, podem ser mencionados senhas, certificados e prazo de uso em um sistema.	Atributos de segurança deverão ter limitação de uso por tempo, de acordo com a política institucional. Dentre os atributos de segurança com validade, podem ser mencionados senhas, certificados e prazo de uso em um sistema. Essa limitação deverá estar alinhada com a política de senhas.
bk		Validade dos atributos de segurança	Quando aplicável, os usuários deverão ser avisados previamente sobre a necessidade de renovação dos atributos de segurança. Esse aviso deverá obedecer à política institucional, ou deverá ser realizado, minimamente, 15 dias antes da expiração. Deverão ser estabelecidos mecanismos de	Os usuários deverão ser avisados previamente sobre a necessidade de renovação dos atributos de segurança. Esse aviso deverá obedecer à política institucional, ou deverá ser realizado, minimamente, 15 dias antes da expiração. Deverão ser estabelecidos mecanismos de renovação automática. Ex.: Troca de senha de acesso.



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			renovação automática.	
bl		Especificação das funções de gerenciamento	Deverá ser criada de forma nativa ou customizada uma lista com todas as funções de gerenciamento de segurança disponibilizadas pelo sistema.	Criar uma lista com todas as funções de gerenciamento de segurança disponibilizadas pelo sistema. Deverá ser possível gerar um relatório com essas permissões.
bm		Regras de gerenciamento de segurança	Deverão ser definidas regras customizadas para auditores, administradores, administradores de segurança e outros usuários.	Deverão estar documentadas todas as regras para cada tipo de perfil. Deverá ser possível gerar um relatório que será utilizado na validação do sistema. Essas regras, após implantadas, devem ter condições de serem auditadas
bn	FPR - Privacidade	Anonimato	Para os acessos públicos, as funções de segurança não poderão guardar rastros dos usuários, preservando, assim, suas identidades perante o sistema e outros usuários.	Para os acessos públicos, as funções de segurança não poderão guardar rastros dos usuários, preservando assim, suas identidades perante o sistema e outros usuários. As evidências de utilização dos sistemas deverão estar registradas somente para fins de auditoria Convém que sejam tomados cuidados para não gravar informações sensíveis. Exemplos: - Gravação em <i>cookies</i> .
bo		Anonimato	Para os acessos públicos, as funções de segurança deverão ser proibidas de solicitar as credenciais do usuário.	Para os acessos públicos, as funções de segurança deverão ser proibidas de solicitar as credenciais do usuário.
bp		Pseudo anonimato	Os usuários deverão ser tratados por referências internas para garantir a possibilidade de auditoria. Somente	Elaborar mecanismo para garantir um identificador único para o acesso anônimo para fins de auditoria. Ex: IP + identificador de sistema



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			auditores poderão ter acesso aos registros de uso do sistema e suas funções por um usuário.	
bq		Restrição à interceptação	As credenciais de acesso nunca poderão trafegar em formato aberto, desprotegido.	É obrigatório o uso de criptografia nas informações de credenciais.
br		Restrição à interceptação	O sistema deverá garantir que as informações dos usuários, bem como dados sigilosos, trafeguem de forma segura, de modo a impedir que usuários não autorizados ou convidados interceptem esses dados.	É obrigatório o uso de criptografia nos dados, empregando os seguintes recursos: - HTTPS (SSL/TLS) - Criptografia na aplicação Esses requisitos restringem, por exemplo, a interceptação com <i>sniffers</i>
bs		Restrição à interceptação	Deverão ser definidos auditores com a capacidade de analisar a utilização de recursos pelos usuários.	Criação obrigatória de perfil específico para auditoria. Esse perfil terá acesso a todos os registros de auditoria. Será de responsabilidade do gestor definir quem será o auditor.
bt	FPT – Proteção das Funcionalidades de Segurança	Falha segura	O sistema deverá tratar as falhas sem exibir os erros e sem fornecer informações que possam ser usadas para exploração de possíveis vulnerabilidades. Dados pessoais e confidenciais nunca deverão ser incluídos em mensagens de erro.	O sistema deverá tratar as falhas sem exibir os erros e sem fornecer informações que possam ser usadas para exploração de possíveis vulnerabilidades. Dados pessoais e confidenciais nunca deverão ser incluídos em mensagens de erro.
bu		Falha segura	Mensagens de erro de sistema	Mensagens de erro de sistema deverão ser exibidas



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			deverão ser exibidas apenas para pessoal autorizado.	apenas para pessoal autorizado.
bv		Segurança nas transferências internas de dados	Os dados manipulados pelo sistema deverão ser sempre mantidos sob o mesmo nível de integridade e confidencialidade exigidos pelo nível de segurança adotado.	Os dados manipulados pelo sistema deverão ser sempre mantidos sob o mesmo nível de integridade e confidencialidade exigidos pelo nível de segurança adotado.
bw		Recuperação confiável	Deverá haver um processo bem definido de recuperação do sistema em caso de falha. Deverão ser definidos responsáveis pela recuperação.	Deverá haver um processo bem definido de recuperação do sistema em caso de falha. Deverão ser definidos responsáveis pela recuperação. Esse processo de recuperação deverá estar alinhado com o plano de continuidade de negócios da SEF/MG.
bx		Recuperação confiável	Deverão ser empregados mecanismos de reversão para a última configuração válida em sistemas de transação.	Criar mecanismos que permitam que o usuário restaure a última configuração válida. Utilizar <i>backups</i> de aplicação, configurações e banco de dados.
by		Recuperação confiável	Deverão ser utilizados sistemas de redundância e supressão de erros em tempo real.	Deverão ser empregados mecanismos de redundância de hardware, energia, sistemas operacionais, links de rede e de sistemas. Este requisito deverá estar alinhado com o plano de continuidade de negócios da SEF/MG. A redundância de energia (por meio de no-break e grupo gerador) e links de rede será provida pela SEF/MG no ambiente onde a solução será instalada.
bz		Carimbos de tempo	Deverão ser empregados mecanismos de carimbo de tempo, com base em	Utilizar NTP na atualização e sincronização de tempo nos servidores.



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			relógios confiáveis.	
ca		Carimbos de tempo	de Recomenda-se o uso de carimbos de tempo com sincronização no horário oficial brasileiro, fornecido pelo Observatório Nacional. Deverão ser observadas as regulamentações do ITI sobre o assunto.	Utilizar TSAs (RFC 3628), Time-Stamp Protocol, RFC 3161 ETSI TS 101861 O serviço de carimbo de tempo deverá estar de acordo com a Resolução nº 58, de 28/11/2008 e demais normas da ICP-Brasil. Verificar homologação das normas de TSA e TSP com o ICP-Brasil.
cb		Consistência de dados	de Deverão ser implementados controles que evitem a edição simultânea de dados.	Este requisito deverá ser tratado dependendo do nível de isolamento. Exemplos: - Campo de versão nas tabelas do SGBD para o caso de transação otimista (modelo de concorrência otimista). - Utilização de bloqueios (<i>locks</i>) para o caso de transação pessimista (modelo de concorrência pessimista). - Dentre os controles, podem ser adotadas medidas em que um usuário possa editar um documento e outros tenham somente acesso de leitura. Cada aplicação deverá possuir a gestão de seus respectivos dados, sendo o compartilhamento feito via serviço.
cc		Consistência de dados	de Controles de replicação deverão ser estabelecidos a partir de uma única origem de dados.	Controles de replicação deverão ser estabelecidos a partir de uma única origem de dados.
cd	FRU – Utilização de Recursos	Tolerância a falhas	de O sistema deverá contar com mecanismos de tolerância a falhas em caso de falha de hardware e/ou energia.	- Deverão ser empregados mecanismos de redundância de hardware, energia, sistemas operacionais. - Este requisito deverá estar alinhado com o plano de continuidade de negócios da SEF/MG. A SEF/MG proverá redundância de energia (por meio de no-break e grupo



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

				gerador) no ambiente onde a solução será instalada.
ce		Tolerância falhas	a	O sistema deverá contar com mecanismos de redundância do ambiente de software e conectividade. - Deverão ser empregados mecanismos de redundância de hardware, energia, sistemas operacionais, links de rede. - Este requisito deverá estar alinhado com o plano de continuidade de negócios da SEF/MG. A SEF/MG proverá redundância de energia (por meio de no-break e grupo gerador) e de links de rede no ambiente onde a solução será instalada.
cf		Tolerância falhas	a	O sistema deverá contar com mecanismos que o mantenham operacional em caso de falha própria. - Deverão ser empregados mecanismos de redundância de hardware, energia, sistemas operacionais, links de rede e de sistema. - Este requisito deverá estar alinhado com o plano de continuidade de negócios da SEF/MG. A SEF/MG proverá redundância de energia (por meio de no-break e grupo gerador) e de links de rede no ambiente onde a solução será instalada.
cg		Prioridade serviço	do	O sistema deverá limitar o uso dos recursos de acordo com a prioridade de execução. Deverá ser criada uma lista de prioridades das funções do sistema. Criar e documentar uma lista de prioridades das funções do sistema e do uso dos recursos. Implementar controles para limitar o uso de recursos de acordo com a prioridade de execução. Exemplo: - Limitar o número de conexões com banco de dados de acordo com a demanda
ch	FTA	Limitação sessão	da	O sistema deverá limitar o escopo da sessão do usuário com base em seus direitos e regras. Exemplo: - Um usuário de direitos restritos não pode navegar em telas administrativas, mesmo que não consiga salvar suas alterações.
ci		Limitações em sessões concorrentes	em	O sistema deverá ter um número limitado de sessões concorrentes, definido com base na O sistema deverá ter um número limitado de sessões concorrentes, definido com base na disponibilidade de recursos do ambiente.



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

			disponibilidade de recursos do ambiente..	
cj	FTA	Limitações em sessões concorrentes	Um usuário poderá ter somente uma sessão por acesso, não sendo permitidas sessões concorrentes.	Um usuário poderá ter somente uma sessão por acesso, não sendo permitidas sessões concorrentes. Essas medidas restringem o compartilhamento de credenciais, que deixariam um usuário sem poder trabalhar, caso outra pessoa utilize seu <i>login</i> .
ck		Bloqueio e encerramento de sessão	As conexões deverão ser encerradas após 30 minutos de inatividade, ou conforme política da SEF/MG.	As conexões deverão ser encerradas após 30 minutos de inatividade, ou conforme política da SEF/MG. A definição desse intervalo de inatividade poderá ser alterada conforme a necessidade ou mediante aplicação de políticas da SEF/MG.
cl		Avisos de acesso	Antes de fornecer acesso à aplicação, deverá ser exibida uma mensagem, informando que: 1. O usuário está acessando um sistema governamental, que deverá ser utilizado de acordo com a legislação vigente; 2. O sistema é monitorado e que, ao acessá-lo, o usuário concorda que algumas de suas ações possam ficar registradas para aplicações legais; 3. O uso não autorizado do sistema é proibido.	Antes de fornecer acesso à aplicação, deverá ser exibida uma mensagem, informando que: 1. O usuário está acessando um sistema governamental, que deverá ser utilizado de acordo com a legislação vigente; 2. O sistema é monitorado e que, ao acessá-lo, o usuário concorda que algumas de suas ações possam ficar registradas para aplicações legais; 3. O uso não autorizado do sistema é proibido. Exemplo: "Este sistema e todos os dados por ele tratados são propriedade da XXXX e devem ser usados exclusivamente para tarefas autorizadas. Caso você não seja usuário autorizado, feche o sistema imediatamente. Usuários autorizados devem conhecer seus direitos no sistema e, mesmo se permitido pelo sistema, não devem acessar dados fora de seus direitos. Todas as ações no sistema são de responsabilidade do usuário que efetuou <i>logon</i> e



				são registradas em trilhas de auditoria”.
cm		Estabelecimento de sessão	De acordo com a política da SEF/MG, o sistema deverá ter restrições de acesso, considerando: 1. Origem do acesso (ex. IP); 2. Horário do acesso (ex. proibido das 19 às 6 h).	De acordo com a política da SEF/MG, o sistema deverá ter restrições de acesso, considerando: 1. Origem do acesso (ex. IP); 2. Horário do acesso (ex. proibido das 19 às 6 h);.
cn		Canais seguros	O sistema deverá estabelecer um canal seguro entre o usuário e suas funções de segurança como, por exemplo, no momento da autenticação.	Conforme regras de negócio da SEF/MG, as informações devem trafegar em canais seguros (SSL)

1.2.2 - ESPECIFICAÇÃO DA IMPLANTAÇÃO

- I. O fornecedor contratado deverá executar o serviço de instalação, configuração e ativação de todos os módulos e funcionalidades, dentro de cronograma a ser estabelecido pela direção da Superintendência de Tecnologia da Informação da SEF/MG, respeitados critérios de viabilidade, disponibilidade da infraestrutura e planejamento.
- II. O serviço de instalação deverá realizar a completa configuração da solução nos servidores e dispositivos necessários, incluindo importação e normalização de dados, geração de conectores e scripts, desenvolvimento de formulários e relatórios, análise e definição de perfis, grupos e workflows em, pelo menos:
 - 8000 usuários ativos; esses dados têm como origem os seguintes sistemas: Active Directory, tabelas de autenticação Unix (/etc/passwd), tabelas de autorização Oracle;
 - os seguintes sistemas e funcionalidades:
 - a) formulário de recuperação ou renovação de senha para, no mínimo, serviços de rede Windows (Active Directory) e correio eletrônico (Exchange Server), e um sistema baseado em banco de dados Oracle 10, servidor de aplicação Oracle Application Server 10.2, arquitetura J2EE, framework Unifw, denominado CADIN, empregando framework J2EE Unifw (desenvolvido pela empresa Unitec, hoje parte da empresa CPM/Braxis);



- b) provisionamento dos sistemas e serviços descritos acima, além de: b1) sistema baseado em banco de dados Oracle, denominado Auditor Web, empregando arquitetura J2EE, servidor de aplicação JBoss, construído sobre a solução de software livre para portais OpenCMS; b2) sistema denominado Auditor Eletrônico, cliente-servidor standalone, para execução em desktop/notebook, construído utilizando IDE Delphi, utilizando banco de dados Firebird e realizando autenticação, para controlar o acesso a alguma de suas funcionalidades, mediante credenciais armazenadas em banco de dados Oracle e; b3) sistema denominado SICAF, baseado em banco de dados Oracle, empregando ambiente Natural (Software AG), com autenticação baseada em usuários do ambiente operacional Solaris 10.
- 10 unidades organizacionais da SEF/MG, geograficamente distribuídas pelo Estado de Minas Gerais;
 - 16 superintendências centrais;
 - os seguintes relatórios:
 - a) todos os sistemas de um usuário (ou grupo de usuários);
 - b) todos os usuários de um sistema ou recurso (ou grupo de sistemas e recursos);
 - c) lista de usuários por categoria, atributos ou direitos associados;
 - d) lista de usuários por *status* (ativo, inativo, desabilitado, bloqueado, suspenso etc.);
 - e) lista de contas que nunca expiram, contas expiradas, contas sem acesso há mais de determinado tempo;
- III. Sem prejuízo das atividades de implantação previstas no item II desta seção 1.2.2, que deverão ser executadas em conformidade com cronograma físico-financeiro contido no contrato, o fornecedor deverá realizar instalação preliminar do software e hardware que compõe a solução, deixando-a em condições de uso, até 120 (cento e vinte) dias após a assinatura do contrato.
- IV. A importação dos dados existentes deve considerar árvores LDAP e perfis distintos de acordo com a origem, buscando a convergência dos identificadores comuns em uma única identidade. A identificação do usuário (*uid*) deverá ser equivalente à do sistema existente, sem gerar impacto em tradução de identificadores nos sistemas de origem.
- V. O serviço de instalação/implantação deverá ser completamente documentado, em termos das especificidades enfrentadas, e a documentação deverá ficar disponível na STI/SEF-MG, em até 15 dias após a conclusão desse serviço.
- VI. A documentação deverá ser completa e suficiente para que o processo de instalação possa ser refeito, sem exceções ou ressalvas.
- VII. A documentação deverá incluir a descrição e mapeamento dos processos relativos à gestão de identidades, como os *workflows* de aprovação e outros, pertinentes aos sistemas e perfis implantados durante o serviço de instalação.
- VIII. A instalação/implantação propriamente dita, conforme descrita acima, deverá ocorrer no prazo máximo de 240 (duzentos e quarenta) dias contados da assinatura do contrato com o fornecedor vencedor.
- IX. O fornecedor deve considerar, ao realizar o planejamento de capacidade para fornecimento do *hardware* (*appliances* ou servidores nos quais os softwares que viabilizam a gestão de identidades serão instalados), os seguintes requisitos:
- a. Possuir capacidade de CPU e memória dimensionados para atingir ocupação máxima de 80% (oitenta por cento) da capacidade instalada, considerando o pior caso, levando em conta a possibilidade de falha de pelo menos um dos equipamentos fornecidos, mesmo que a solução suporte balanceamento de carga; assim, deverá ser considerado que 1 equipamento terá utilização máxima de CPU e memória de 80%, suportando o funcionamento de toda a solução, caso sejam



fornecidos 2 equipamentos; caso sejam fornecidos 3 equipamentos, o referido dimensionamento deverá levar em conta 2 equipamentos, tendo em vista a possibilidade de falha de 1 deles, e assim sucessivamente;

- b. Os equipamentos fornecidos (*appliances* ou servidores) devem ser novos, de primeiro uso e estar em linha de produção do fabricante no momento da entrega;
- c. Os equipamentos fornecidos devem ser montados em rack 19" (fornecido com o kit de montagem).
- d. A solução deverá ser redundante, isto é, deverão ser fornecidos pelo menos 2 (dois) equipamentos, configurados para prover alta disponibilidade, a fim de permitir tolerância a falhas, em modo ativo-passivo ou ativo-ativo;

- X. O fornecedor deverá se responsabilizar, também, pela instalação do cabeamento lógico e elétrico para *appliances* ou servidores onde será processada a solução. A instalação do cabeamento lógico deverá ser feita utilizando cabeamento de par trançado não-blindado (UTP) categoria 6 e 6A, com *patch cords* que deverão ser da categoria 6 e, se for o caso, fibras ópticas multimodo e passivos de rede, ambos com tecnologia Systimax, a fim de preservar a certificação do ambiente onde os equipamentos serão instalados, para todos os pontos lógicos necessários ao funcionamento da solução. O fornecedor será responsável, também, pelo detalhamento da execução, tomando como referência projeto básico indicativo elaborado pela SEF. Será de sua responsabilidade, ainda, a obtenção de aprovação para o serviço de instalação a ser efetuado, a ser concedida pela empresa responsável pela construção do *datacenter* da SEF e por sua manutenção, a fim de garantir a manutenção da certificação pela norma ABNT NBR 15247. A instalação elétrica deverá empregar os mesmos padrões adotados hoje no *datacenter* da SEF, particularmente no ambiente de sala-cofre, a saber, cabos multipolares do tipo Afumex (PRYSMIAN), isolamento para 750 V, seção mínima de 4,0 mm², nas cores preto (fase), azul (neutro) e verde (terra); tomada tipo 2P+T pino chato (fase, neutro e terra) 15 A – 127 V ou tomada tipo 3P pino chato (fase, fase e terra) 20 A – 220 V, conforme a tensão, devendo todas as tomadas ser identificadas por meio de etiquetas legíveis e indelévels fixadas nas tampas das caixas; disjuntores de proteções dos circuitos eletromagnéticos monopolares, bipolares e tripolares, conforme a norma ABNT/NBR-NM 60898 e no padrão IEC (DIN), fixados pela base por engate rápido sobre trilho, respeitando ou reforçando as performances do sistema na coordenação, possuindo capacidade de interrupção, Icn, aquecimentos para maior segurança, continuidade de serviço (seletividade) ou otimização econômica (filiação).

1.2.3 - LICENCIAMENTO DO SISTEMA DE GESTÃO DE IDENTIDADES E ACESSO

- I. O sistema deverá ser licenciado na sua versão comercial mais atual.
- II. Deverão estar cobertos pela aquisição, assim como deverão ser licenciados, todos os módulos e funcionalidades exigidos para atendimento à especificação do objeto – item 1 deste Termo de Referência.
- III. A aquisição da solução implicará em licenciamento para uso contínuo, permanente e por tempo indeterminado do sistema e também das quantidades de identidades contratadas nos termos deste Termo de Referência.
- IV. O licenciamento da solução deverá incluir:
 - uma população estimada em 8.000 identidades ativas, em uso, em termos de contas de usuário e contas setoriais de correio eletrônico do Microsoft Active Directory e Exchange Server, com acesso efetivo a um ou mais sistemas, incluindo autenticação na rede de computadores, entre as quais se incluem:
 - a) 6.000 identidades de servidores efetivos, estatutários e celetistas, e cargos em comissão;
 - b) 800 contas de correio eletrônico setorial, com utilização de serviços do Active Directory e do Exchange Server;
 - c) 1.200 identidades relativas a estagiários, cedidos, prestadores de serviço e colaboradores de outras formas de provimento.



- quantidade ilimitada de grupos, perfis, workflows e demais objetos de controle e automação internos da solução, bem como quantidade ilimitada de sistemas integrados;
- compatibilidade nativa às tecnologias estabelecidas no item 1 – Objeto;
- a quantidade necessária de instalações lógicas e físicas em servidores, computadores e outros dispositivos, a fim de atender à estrutura da SEF/MG.
- garantia de atualização do sistema e de suporte técnico pelo fabricante, válida por 48 (quarenta e oito) meses, na forma definida no item 1.2.5 abaixo, período em que poderá haver adequação de valores, conforme a quantidade efetiva de usuários, nos termos da lei.

1.2.4 - ESPECIFICAÇÃO DO TREINAMENTO

O contratado deverá ministrar treinamento aos funcionários da SEF-MG da forma indicada a seguir:

- I. O objetivo do treinamento é assegurar a transferência de conhecimento na instalação, configuração, administração, adaptação, parametrização, ajuste (customização) e uso da ferramenta em todos os recursos, funcionalidades e requisitos especificados.
- II. O treinamento será conduzido por meio de aulas expositivas e práticas.
- III. O treinamento será ministrado na cidade de Belo Horizonte, às expensas do fornecedor contratado, inclusive no que se refere à disponibilização de local/instalações para sua realização e no que diz respeito aos recursos instrucionais, tais como *datashow* e computadores, caso necessários.
- IV. O material didático deverá ser fornecido em mídia impressa e mídia eletrônica em formatos padrão de mercado (PDF, DOC, PPT ou HTML) no idioma português do Brasil ou inglês.
- V. Todas as despesas decorrentes do treinamento, tais como alocação de instrutores, confecção do material didático, bem como as despesas com deslocamento, hospedagem e alimentação dos instrutores, serão de responsabilidade do fornecedor contratado.
- VI. O fornecedor contratado, deverá prover treinamento específico, amplo e aprofundado, conforme definido abaixo:
 - a. curso de 20h/aula, para até 12 (doze) treinandos, principalmente administradores, gerentes e técnicos das áreas de suporte técnico e infraestrutura, designados para participar do treinamento pela STI/SEF-MG, sobre a instalação da solução e seus módulos e configurações básicas, a ser ministrado antes da execução do serviço de instalação;
 - b. curso de 20h/aula, para até 12 (doze) profissionais de desenvolvimento de sistemas, designados para participar do treinamento pela STI/SEF-MG, sobre a elaboração de conectores, consultas e integração em geral, a ser ministrado antes da execução do serviço de instalação;
 - c. curso de 40h/aula, para até 30 (trinta) treinandos, principalmente futuros administradores e gestores oriundos de diversas áreas, sobre o processo de operação normal da ferramenta, incluindo gestão de perfis, identidades, workflows e formulários, entre outros, a ser ministrado após a execução do serviço de instalação.
 - d. curso de 4h/aula, para até 12 (doze) treinandos, principalmente futuros gestores e usuários, a fim de estabelecer multiplicadores, sobre o processo de operação normal da solução, incluindo requisições, aprovações e notificações, recuperação de senhas e outros, a ser ministrado para 10 turmas, após a execução do serviço de instalação.



- VII.** O fornecedor contratado deverá fornecer material didático sobre os cursos ministrados, em forma de apostilas ou livretos, impressos e em meio digital, sendo que, para os cursos ministrados após a execução do serviço de instalação, o conteúdo deverá apresentar telas e textos em conformidade com a configuração e personalização empregada, para ilustrar casos reais de uso.
- VIII.** Todo o processo de treinamento deverá ser submetido à avaliação por parte dos funcionários indicados pela SEF/MG.
- Caso a avaliação seja considerada insatisfatória, na média das avaliações, caberá à SEF/MG julgar se caberá:
 - a) reedição, total ou parcial, dos cursos, em data a ser definida;
 - b) não pagamento, total ou proporcional, referente aos cursos não aprovados.
- IX.** O contratado deverá prover certificados de participação aos espectadores com frequência superior a 75%, individuais e nominativos, nos cursos homologados pela SEF/MG.
- X.** Os serviços de treinamento deverão ser executados em até 300 (trezentos) dias contados da assinatura do contrato.
- XI.** Após a conclusão satisfatória do treinamento e emissão dos certificados correspondentes, na forma prevista no subitem **IX** acima, será expedido Termo de Aceite Técnico pela SEF, referente ao treinamento.

1.2.5 – ESPECIFICAÇÃO DA GARANTIA

- I) A garantia é constituída pelas seguintes atividades:
- a. Suporte técnico e manutenção corretiva da ferramenta compreendendo o diagnóstico e identificação de problemas, correção de erros, defeitos (*bugs*) ou mal-funcionamento sobre qualquer funcionalidade ou decorrente de qualquer customização efetuada pelo contratado durante a fase de implantação, atendendo ao chamado expresso da STI/SEF, visando o restabelecimento do funcionamento dos serviços, quando da ocorrência de quaisquer falhas ou problemas de ordem técnica..
 - b. Atualização da ferramenta, incluindo correções (*patches*), liberações (*releases*) e versões (*versions*).
 - c. Suporte técnico e manutenção corretiva dos *appliances* ou servidores (*hardware*), incluindo substituição de peças e mão de obra, também com vistas ao restabelecimento do funcionamento dos serviços.
- II. O suporte técnico será solicitado mediante chamada telefônica da SEF/MG ou por site Web ou, ainda, por e-mail, cujos meios de contato deverão ser informados pelo fornecedor contratado para que este, por meio de seu representante técnico, corrija as falhas apresentadas, colocando os serviços em plenas condições de operação.
- III. Deverá ser fornecido à SEF-MG um número de telefone que possibilite ligações locais em Belo Horizonte/MG ou interurbanas gratuitas para a central de suporte técnico (tipo 0800), para fins de abertura e acompanhamento de chamados.
- IV. O serviço de suporte prestado na modalidade *web* e *e-mail* deverá estar disponível para abertura e acompanhamento de chamados de *software* e *hardware* em tempo integral (24 horas por dia, sete dias por semana, todos os dias do ano, inclusive sábados, domingos, feriados e pontos facultativos). Dessa forma, a qualquer hora do dia ou da noite, a SEF-MG terá acesso aos recursos on-line de que precisa para baixar correções e atualizações de software a que tem direito, com novas funcionalidades e aperfeiçoamentos, além de ter acesso às correções de falhas em geral e de segurança do software.



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

- V. Não deverá haver qualquer limitação para o número de solicitações de suporte de software, assim como não deverá haver qualquer limitação para o número de técnicos da SEF-MG autorizados, mediante indicação da Secretaria, a abrir chamados técnicos de software.
- VI. Ao abrir um chamado relacionado a *software*, a SEF-MG, de comum acordo com a CONTRATADA, poderá classificá-lo em 4 (quatro) níveis de severidade:
- Severidade CRÍTICA: é uma condição de emergência que paralisa a execução de qualquer módulo, componente ou utilitário do software que compõe a solução, impedindo assim a utilização contínua de qualquer um dos recursos ou funcionalidades especificados neste edital, sejam eles nativos ou adaptados (customizados) pela CONTRATADA.
 - Severidade ALTA: é uma condição em que um erro ou problema severo causa uma grave perda do potencial operacional do software que compõe a solução ou paralisa totalmente uma funcionalidade crítica em sua operação. Nesse caso, mesmo que não esteja disponível nenhuma *solução de contorno* para o problema em questão, a operação da solução pode continuar de modo restrito.
 - Severidade MÉDIA: a condição correspondente ao nível de severidade média ocorre, tipicamente, a partir de um erro detectado em uma funcionalidade do software que compõe a solução, que dificulta seus usuários na condução de suas atividades, embora existam alternativas disponíveis para tal. Geralmente a origem são problemas pontuais que envolvem poucos usuários.
 - Severidade BAIXA: a condição correspondente ao nível de severidade baixa não refere-se a perda de funcionalidade do software que compõe a solução, e portanto não cria nenhum impacto grave em sua operação. Os chamados para esta categoria de severidade podem tratar de requisição de informações, melhorias ou esclarecimentos relativos à funcionalidade e documentação da solução.
- VII. O serviço de suporte prestado por telefone para software deverá estar disponível para abertura e acompanhamento de chamados, conforme os períodos definidos para o nível de severidade dos chamados, conforme item VIII) abaixo.
- VIII. Os períodos de disponibilidade do serviço de suporte técnico de software, para registro de chamados por telefone, são:
- Severidade CRÍTICA: 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano, inclusive sábados, domingos e feriados.
 - Severidade ALTA: 08:30 às 17:30 horas, em dias úteis (2ª a 6ª Feira).
 - Severidade MÉDIA: 08:30 às 17:30 horas, em dias úteis (2ª a 6ª Feira).
 - Severidade BAIXA: 08:30 às 17:30 horas, em dias úteis (2ª a 6ª Feira).
- IX. O registro de chamados de suporte técnico de hardware deverão estar disponíveis 24 horas por dia, 7 dias por semana, inclusive sábados, domingos e feriados.
- X. O serviço de atendimento do fornecedor contratado deverá informar à SEF/MG, no mínimo, o nº identificador do chamado, bem como a data e hora e a previsão de atendimento.
- XI. O fechamento de cada atendimento pela CONTRATADA só poderá ser efetuado após a anuência formal da SEF-MG.
- XII. Após o término do atendimento, isto é, fechamento do chamado, deverá ser fornecido laudo técnico ou relatório de atendimento contendo, no mínimo, o nº identificador do chamado, bem como a data e hora do chamado, data e hora do início e do término do atendimento, identificação do problema e solução aplicada.
- XIII. O laudo técnico ou relatório de atendimento deverá ser, preferencialmente, disponibilizado pelo fornecedor para a SEF-MG em um sítio (*site*) web com acesso controlado por senha, ou enviado para a SEF-MG através de mensagem eletrônica (*email*).



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

- XIV. O fornecedor contratado deverá apresentar prazo de garantia, contra falhas ou defeitos de qualquer natureza na execução dos serviços de, no mínimo, 04 (quatro) meses, contados a partir da entrega dos produtos tangíveis.
- XV. Visando garantir a efetividade do atendimento relativo à manutenção e suporte técnico, o fornecedor deve manter sempre atualizados junto à SEF-MG os meios de comunicação com a Central de Atendimento própria ou do fabricante.
- XVI. Em todas as atividades de assistência técnica ou suporte relacionadas à garantia dos produtos, os técnicos do fornecedor vencedor deverão empregar a língua portuguesa, exceto no uso de termos técnicos e na utilização de textos técnicos, que poderão estar redigidos em Inglês.
- XVII. Deverá ser garantido à SEF-MG, sem qualquer ônus adicional, o pleno acesso aos sites dos fabricantes dos produtos ofertados, mediante controle de acesso por senha, com direito a consultas a quaisquer bases de dados disponíveis para usuários, e também efetuar downloads de quaisquer atualizações de software ou documentação.
- XVIII. O suporte técnico será prestado pelo fornecedor ou fabricante. No caso do fornecedor não ser o próprio fabricante da solução fornecida – software e hardware – deverá provar de forma inequívoca a contratação da garantia estendida junto ao fabricante transferível à SEF-MG ou apresentar declaração do fabricante concordando com todas as exigências da garantia exigida, específica para este processo, antes da assinatura do contrato.
- XIX. O fornecedor deverá designar um profissional responsável pelo acompanhamento das solicitações de suporte abertas pela SEF-MG. Caberá a esse profissional supervisionar os técnicos do fornecedor responsáveis pelo atendimento dos chamados abertos pela SEF-MG. Esse profissional será o contato oficial da SEF-MG com o fornecedor para assuntos relativos ao suporte técnico. A comunicação com esse profissional será realizada obrigatoriamente no idioma português do Brasil.
- XX. As atualizações de software e de base de conhecimento de segurança deverão estar disponíveis, preferencialmente, na modalidade de *live update*, ou em até 03 (três) dias para qualquer outro mecanismo de atualização das versões, durante todo o período de garantia. Ao final do prazo de garantia, a SEF-MG terá direito às licenças de uso dos *softwares* por tempo indeterminado, na última versão disponível quando do término da garantia.
- XXI. O serviço de suporte técnico deverá estar disponível para utilização após o recebimento da solução e deverá permanecer disponível para utilização até o fim da vigência da garantia.
- XXII. Conceitua-se solução de contorno, neste anexo, como sendo uma solução temporária para um problema que não elimina a sua causa-raiz, mas que reduz o impacto para as pessoas potencialmente afetadas pelo problema. No caso específico de um problema de mau funcionamento ou defeito em um software, a solução de contorno restabelece a disponibilidade, ainda que parcial, do software com problema, possibilitando assim a execução de suas funções principais. No caso de um chamado de suporte técnico, a solução de contorno altera o estado (*status*) do chamado de “pendente” para “contingenciado”.
- XXIII. Conceitua-se solução definitiva, neste anexo, como sendo uma solução que elimina definitivamente a causa-raiz de um problema. No caso de um chamado de suporte técnico, a solução definitiva altera o estado (*status*) do chamado para “resolvido”, e o chamado pode ser então encerrado.
- XXIV. Conceitua-se causa-raiz, neste anexo, como sendo um fato que originou um determinado problema, o que é conceitualmente diferente da consequência do problema. Assim sendo, a interrupção ou travamento da execução de determinado software, por exemplo, não é a causa raiz. A execução de um código incorreto ou a existência de problemas da integração desse software com o sistema operacional hospedeiro podem ser a causa raiz de tal interrupção ou travamento.



- XXV. Será expedido Termo de Aceite Técnico de garantia, referente ao software e ao hardware, tão logo seja concluído recebimento desses dos equipamentos (*appliances* ou servidores), bem como do software de gestão de identidades, e realizada a instalação e a configuração iniciais. A emissão desse Termo também ficará condicionada à verificação da efetiva possibilidade de abertura de chamado de suporte técnico para o software e para o hardware que compõem a solução.

1.2.5.1 – Especificação do Nível de Serviço da Garantia

- I. Os níveis de serviço para os chamados de suporte técnico para software são:
 - a. Severidade CRÍTICA: a CONTRATADA deverá apresentar uma *solução de contorno* em até 4 (quatro) horas corridas e uma *solução definitiva* em até 10 (dez) dias corridos, a partir da hora de abertura do chamado. Caso não seja apresentada uma *solução de contorno* no prazo estipulado, o suporte técnico deverá ser *on-site* e a *solução de contorno* não poderá ultrapassar 8 (oito) horas corridas.
 - b. Severidade ALTA: a CONTRATADA deverá apresentar uma *solução de contorno* em até 8 (oito) horas úteis e uma *solução definitiva* em até 15 (quinze) dias úteis, a partir da hora de abertura do chamado.
 - c. Severidade MÉDIA: a CONTRATADA deverá apresentar uma *solução de contorno* em até 40 (quarenta) horas úteis e uma *solução definitiva* em até 20 (vinte) dias úteis, a partir da hora de abertura do chamado.
 - d. Severidade BAIXA: a CONTRATADA deverá apresentar uma resposta em até 5 (cinco) dias úteis, a partir da hora de abertura do chamado.
- II. Os níveis de serviço para atendimento de chamados relacionados a *hardware* (*appliances* e servidores) envolvem resposta aos chamados telefônicos em até 4 (quatro) horas e atendimento *on-site*, para os casos em que houver necessidade da presença de técnico no local, no próximo dia (até 24 horas corridas após solicitação da SEF/MG), e com prazo de solução de até 48 (quarenta e oito) horas a partir do registro do chamado.
- III. Considera-se hora útil aquela compreendida no horário de 08:00 às 20:00 horas, em dias úteis, de segunda a sexta feira.
- IV. O não atendimento de um chamado de suporte dentro do prazo máximo definido, segundo o nível de severidade, para software, e independentemente desse fator, para hardware, ensejará aplicação de multa à CONTRATADA no valor correspondente a 0,3 % (três décimos por cento) sobre o valor total do CONTRATO, por cada dia de atraso (ou fração) referente a chamado não atendido no prazo ou 20% (vinte por cento) sobre o valor total do CONTRATO, em caso de atraso superior a 30 (trinta) dias. O valor de multa eventualmente devido pela CONTRATADA poderá ser descontado da próxima fatura.

1.2.6 – ESPECIFICAÇÃO DOS SERVIÇOS DE COACHING/MENTORING

- I. O fornecedor deverá prestar, sob demanda até 1.000 (mil) horas de serviços, envolvendo o acompanhamento *in loco*, objetivando o desenvolvimento e *coaching/mentoring* no uso, suporte e gestão da solução, da forma indicada nas demais alíneas abaixo.
- II. O serviço de *coaching/mentoring* consiste no acompanhamento, orientação e esclarecimento de dúvidas por pelo menos um membro da equipe técnica do fornecedor aos usuários da solução indicados pela SEF-MG.
- III. A critério da SEF-MG, poderá ser exigida a participação simultânea de até 3 (três) técnicos do fornecedor em cada demanda de *coaching/mentoring*.
- IV. Faz parte do escopo das atividades de *coaching/mentoring*:
 - a) Orientação e transferência de conhecimento quanto ao uso, suporte e gestão da solução, visando otimizar a produtividade dos profissionais e garantir a qualidade dos artefatos gerados pela solução;



- b) Orientação quanto à customização da solução, visando suportar a execução do(s) processo(s) de software desejado(s) pela SEF-MG; e
 - c) Orientação quanto à integração da solução às soluções, tecnologias e produtos de software existentes na SEF-MG e em outros órgãos ou entidades da Administração Pública de Minas Gerais.
- V. A execução das atividades de *coaching/mentoring* será realizada por demanda e não há obrigação da SEF-MG em executá-las integralmente.
- VI. A duração mínima de cada demanda de *coaching/mentoring* será de 16 horas (dezesesseis horas) úteis, ou seja, 2 (dois) dias corridos, definidos em conjunto pela SEF-MG e o fornecedor.
- VII. As horas previstas para *coaching/mentoring* deverão ser alocadas ao longo do período de 12 (doze) meses, contado da assinatura do contrato.
- VIII. As atividades de *coaching/mentoring* deverão estar subordinadas a solicitações de abertura e relatórios de fechamento destes tipos de serviço, considerando sempre uma solicitação prévia formal da SEF-MG e posterior aceite das atividades realizadas. Tais procedimentos serão acordados no início da utilização deste tipo de atividade.
- IX. O fornecedor deverá apresentar, até o quinto dia útil de cada mês, relatório contendo as atividades de *coaching/mentoring* realizadas no mês anterior. Este relatório deverá apresentar, no mínimo, as seguintes informações: nome dos executantes das atividades, perfil dos profissionais, descrição das atividades, a quantidade de horas e o valor a ser recebido.
- X. O relatório mensal contendo as atividades de *coaching/mentoring* deverá ser assinado pelo responsável indicado pelo fornecedor para acompanhamento e interlocução do contrato.
- XI. As atividades de *coaching/mentoring* deverão ocorrer em instalações da SEF/MG, localizadas na Região Metropolitana de Belo Horizonte, nos dias úteis (2ª a 6ª Feira), no horário de 08:30 às 18:00 horas.
- XII. É de responsabilidade do fornecedor o deslocamento de técnicos para a execução das atividades de *coaching/mentoring*, sem ônus adicional para a SEF-MG.
- XIII. Os profissionais do fornecedor deverão possuir qualificação técnica apropriada para exercer as atividades de *coaching/mentoring*. Exige-se que os profissionais possuam treinamentos especializados em um ou mais módulos da solução, de acordo com a alocação do profissional nas atividades de *coaching/mentoring*, bem como experiência na realização de atividades de cunho similar (*coaching/mentoring*). Os treinamentos especializados deverão ser comprovados por certificação emitida pelo fabricante da solução ou por entidade credenciada pelo fabricante a fazê-lo, condição que será verificada no momento da assinatura do contrato.

1.2.7 – CONSIDERAÇÕES GERAIS

I – Neste anexo, dentro do contexto da especificação de requisitos, considera-se como:

- a) **nativa**, qualquer funcionalidade que já esteja disponível no conjunto de software adquirido como parte da solução e cujos componentes são do mesmo fabricante, requerendo apenas parametrizações para que possa ser usada;
- b) **nativa customizada**, qualquer funcionalidade que demande esforço de programação para sua disponibilização, usando para isso, porém, apenas recursos, tais como interfaces de programação da aplicação – APIs, disponibilizados pelo software fornecido como parte da solução, de um mesmo fabricante.
- c) **customizada não-nativa**, qualquer funcionalidade que demande esforço de programação para sua disponibilização, mas que requeira o uso de software de terceiros, além do fabricante, para sua implementação.



II - Neste anexo, dentro do contexto da especificação de requisitos, considera-se que todas as funcionalidades descritas na especificação devam ser fornecidas ativas e licenciadas. As exceções estão consignadas de maneira explícita na especificação como sendo objeto de contratação futura.

III – Caso seja permitido o atendimento de requisito presente na especificação técnica contida neste anexo mediante customização, o fornecedor será responsável por efetuar-la, sem quaisquer ônus adicionais para a SEF/MG.

2 – CRITÉRIOS DE ACEITABILIDADE DO LOTE ÚNICO

2.1 - O processo de aceite técnico compreenderá duas fases, a saber, recebimento, com emissão do respectivo Termo de Recebimento, e aceitação técnica, com emissão dos respectivos Termos de Aceite Técnico, conforme descrito nos itens 2.2 e 2.3 a seguir.

2.2 - Recebimento

- a) O fornecedor deverá efetuar visita técnica prévia ao local de entrega, no máximo em 5 (cinco) dias úteis após a assinatura do contrato, para definição de toda a logística para prestação dos serviços, inclusive instalações lógicas e elétricas, identificando portas de rede livres em ativos de rede da Secretaria (switches), envolvendo, inclusive, além da rede local, conectividade com Storage Area Network (SAN), para atendimento das necessidades de armazenamento. Deverá, também, tomar conhecimento do projeto básico das instalações elétricas e lógicas que deverá executar, providenciando seu detalhamento e execução.
- b) O fornecedor deverá acondicionar e transportar as mídias de software que compõe a solução e os equipamentos em embalagem apropriada para o transporte, de acordo com as melhores práticas do mercado e recomendações do fabricante. A embalagem deverá ser identificada com, no mínimo, as seguintes informações:
 - a. Nome do fabricante e marca do produto.
 - b. Número de série ou equivalente.
 - c. Número do pedido de compra.
- c) Todas as licenças de software de software que compõem a solução deverão ser fornecidas com as respectivas mídias de instalação e documentação correspondente.
- d) Os equipamentos (appliances ou servidores) deverão ser fornecidos com a respectiva documentação e com as mídias dos softwares básicos nele instalados (sistemas operacionais, por exemplo).
- e) Todas as licenças de software fornecidas deverão ser permanentes, podendo os respectivos programas ser utilizados por tempo indeterminado pela SEF-MG, independente de prazos de vigência de contratos de manutenção e suporte técnico.
- f) Todas as licenças de software que compõe a solução deverão ser fornecidas com a documentação comprobatória do direito de utilização do software.
- g) A SEF-MG emitirá “Termo de Recebimento” para as licenças de software dos produtos adquiridos e para os equipamentos (hardware – *appliances* ou servidores), atestando, ou não, a conformidade da entrega em relação aos requisitos de licenciamento especificados, aponto recibo na Nota Fiscal (1ª e 2ª vias), caso constatada conformidade.
- h) A emissão do “Termo de Recebimento” para os softwares e hardwares que compõem a solução ficará condicionada à verificação de teste de acesso para registro de chamado de suporte técnico e à realização da instalação preliminar do software e do hardware que compõem a solução, de que trata o sub-item III do item 1.2.2.

2.3 - Aceitação Técnica

- a. O aceite da solução estará condicionado à emissão do respectivo “Termo de Aceite Técnico”, a ser emitido por profissionais designados pela SEF-MG, e ocorrerá após a conclusão das etapas seguintes:
 - I. Recebimento, conforme definido no item 2.2 deste Anexo.
 - II. Instalação, configuração e implantação da solução, conforme definido no item 1.2.2 deste Anexo .
- b. A adequação dos serviços de *coaching* será verificada mensalmente, caso tenham sido consumidas horas da atividade de *coaching* no mês anterior. O aceite dos serviços de



coaching será efetuado mediante a apresentação pelo fornecedor do relatório mencionado no subitem IX) do item 1.2.6 deste anexo e estará condicionado à emissão do respectivo “Termo de Aceite Técnico” pelo fiscal do contrato, que ocorrerá no prazo máximo de 5 (cinco) dias úteis após a entrega desse relatório.

- c. A adequação dos serviços de treinamento será verificada após a realização de cada módulo de treinamento. O aceite dos serviços de treinamento será efetuado mediante a apresentação pelo fornecedor de relatório com a descrição do(s) módulo(s) ministrado(s) e das horas consumidas no treinamento, condicionada à emissão do respectivo “Termo de Aceite Técnico” pelo fiscal do fornecedor, que ocorrerá no prazo máximo de 5 (cinco) dias úteis após a entrega desse relatório e dos certificados mencionados no subitem IX) do item 1.2.4 deste anexo.
- d. A adequação da garantia, que engloba o suporte técnico, será verificada mediante teste do acesso para registro de chamado de suporte para o software e o hardware que compõem a solução, efetuado após o recebimento, sendo expedido o correspondente Termo de Aceite Técnico, caso esse teste seja bem-sucedido,
- e. A participação ou presença de profissionais da SEF-MG, na aceitação técnica não elide a responsabilidade do fornecedor.
- f. Caso os *softwares*, equipamentos ou serviços sejam recusados, por serem diferentes do especificado ou apresentarem defeitos, a sua correção/substituição deverá ocorrer no prazo máximo de 10 (dez) dias úteis, para os softwares e serviços, e 30 (trinta) dias úteis, para os equipamentos, contados da notificação a ser expedida pela SEF/MG, não sendo lavrados os respectivos Termos de Aceite Técnico.
- g. No processo de aceite técnico poderá ser requerida a presença de representante do fornecedor para dirimir as dúvidas da equipe técnica responsável pelo processo.
- h. Na hipótese de os produtos/serviços apresentarem irregularidades não sanadas, será reduzido a termo o fato e encaminhado à autoridade competente, para procedimentos inerentes à aplicação das penalidades.
- i. O prazo de garantia para as licenças de software que são objeto deste contrato será de 48 (quarenta e oito) meses. Esse prazo de garantia será contado a partir da instalação e configuração iniciais dos equipamentos e softwares fornecidos, que se dará até 120 (cento e vinte dias) contados da assinatura do contrato.
- j. Os Termos de Aceite Técnico mencionados nesta seção conterão descrição sucinta do produto ou serviço disponibilizado, número e data da nota fiscal.

3 – DA JUSTIFICATIVA DA CONTRATAÇÃO

Esta contratação justifica-se em razão da necessidade de se adquirir uma solução para gerenciamento de identidades e de acessos, conforme a exposição de motivos constante na Nota Técnica N.º. 42/2011, de 23/05/2011 (anexa ao processo), emitida pela Superintendência de Tecnologia da Informação – STI/SEF.

3.1 - Benefícios

A aquisição de uma solução de gerenciamento de identidades e acessos possibilitará:

- a integração de várias aplicações que fazem uso de diversas bases de usuários, nem sempre sincronizadas e consistentes (estejam estas baseadas em bancos de dados



corporativos ou serviços de diretórios – *Active Directory*), a uma solução de gerenciamento de identidade com um repositório de usuários sincronizado e consistente;

- o mapeamento de processos, a definição de perfis e a definição de políticas de controle de acesso adequadas a cada tipo de negócio e usuário;
- a consolidação do provisionamento de identidades para as diversas bases de autenticação utilizadas pelos recursos conectados à solução por meio de interfaces de uma única solução;
- a centralização e automatização da administração de identidades, ou seja, uma única interface administrativa, com um repositório central de usuários, aumentando assim a segurança e reduzindo os custos através da administração, controle e auditoria;
- o controle e a concessão de acesso para os serviços e sistemas críticos disponibilizados pela SEF/MG e definidos para cada tipo de perfil;
- a auditoria dos eventos de acesso que ocorrerem para cada identidade.

Além dos benefícios para o ambiente computacional da SEF/MG expostos acima, a aquisição de uma solução de gerenciamento de identidades e acessos proporcionará um aumento da produtividade e do nível de satisfação dos usuários, facilidade nos processos de revisão de direitos de acesso, soluções para garantir a conformidade com as políticas, normas e regulamentos de segurança e eliminação do risco de acesso não autorizado ou inapropriado, em função de mudanças de atividades e manutenção do acesso de pessoas que já foram desligadas da SEF/MG. Por fim, a seleção de uma solução de gestão de identidades pela SEF/MG permitirá estabelecer um padrão tecnológico para gerir identidade na administração pública estadual em Minas Gerais, aprimorando a segurança da informação no executivo mineiro.

4 – PROVA DE CONCEITO/AMOSTRA

4.1- O Licitante vencedor, antes da assinatura do contrato, também deverá, a critério da Administração, realizar prova de conceito/ amostra do software ofertado, a fim de comprovar que atende integralmente a todos os requisitos definidos nas especificações técnicas contidas neste anexo, no prazo de 5 (cinco) dias úteis, contados a partir da declaração do vencedor do certame.

4.1.1 - A aprovação da prova de conceito/ amostra do software a ser apresentado pelo Licitante, dar-se-á mediante Termo de Aprovação emitido por comissão avaliadora composta por servidores designados pela STI/SEF-MG para essa função;

4.1.2 A prova de amostra consistirá na apresentação da solução contratada, e terá duração de até 3 (três) dias úteis, podendo ser prorrogada em função da necessidade de se comprovar o atendimento de todos os requisitos técnicos ou a critério da comissão avaliadora;

4.1.3 Os requisitos cuja especificação permitir que sejam atendidos mediante adaptações (customizações) da solução, não precisarão ser demonstrados na prova de amostra, sendo obrigatória a demonstração, contudo, quando for exigido que a solução atenda nativamente ao requisito.

4.1.4 Cada dia da prova de amostra será constituído por 2 (duas) sessões de apresentação, a primeira ocorrendo de 09:00 às 12:00 horas e a segunda de 14:00 às 17:30 horas. O horário poderá ser alterado de comum acordo entre a LICITANTE e a SEF-MG.

4.1.5 O local da prova de amostra é de responsabilidade da LICITANTE, mas deverá estar localizado na Região Metropolitana de Belo Horizonte.

4.1.6 O fornecimento da infraestrutura necessária para a prova de amostra é de inteira responsabilidade da LICITANTE. Todos os custos para a prova de amostra (técnicos da



LICITANTE, infra-estrutura necessária, local de apresentação) serão de exclusiva responsabilidade da LICITANTE, sem ônus para a SEF-MG.

4.1.7 A LICITANTE deverá enviar à SEF-MG, em até 2 (dois) dias úteis antes do início da prova de amostra, uma agenda detalhada da apresentação, com roteiros que listem os requisitos da especificação técnica que serão comprovados em cada sessão da apresentação.

4.2- Caso o Licitante vencedor, sujeito a realização da prova de conceito/ amostra for reprovado, a SEF/MG chamará o segundo colocado no certame, e assim, sucessivamente.

5 – DA AVALIAÇÃO DE CUSTO (Consulta Pública prévia)

Atendendo ao disposto no artigo 6º, alínea “e” do Decreto nº. 44.786, de 18 de abril de 2008, foi procedida consulta de mercado pela Superintendência de Tecnologia da Informação – STI, para verificação dos preços e a estimativa dos custos, baseada no objeto da presente licitação.

6 – DA METODOLOGIA

O critério de julgamento e aceitação das propostas será **MENOR PREÇO GLOBAL OFERTADO PARA O LOTE ÚNICO** e de acordo com as especificações descritas no objeto deste edital.

7 - DA ACEITABILIDADE DA PROPOSTA

Para decisão quanto à aceitabilidade da proposta, o Pregoeiro examinará a melhor classificada, no que se refere à compatibilidade do preço ofertado com o valor estimado para a contratação e com as especificações técnicas do objeto.

8 - DA DOTAÇÃO ORÇAMENTÁRIA

As despesas decorrentes da contratação correrão por conta das dotações orçamentárias n.ºs. 1191.04.129.029.1248.0001.3390.39, fonte 10 e/ou 25.1 e/ou 1191.04.129.029.1248.0001.4490.52., fonte 10.1 e ou 25.1, consignadas na Lei Orçamentária Anual (LOA) que for aprovada para o exercício de 2012, ou no Projeto de Lei Orçamentária Anual (PLOA) 2521/2011, publicado no Diário do Legislativo em 06 de outubro de 2011, encaminhado pela Mensagem do Governador nº 125/2011, de 29 de setembro de 2011, caso este não seja sancionado até o dia 31 de dezembro de 2011, conforme autorizado pelo art. 53, inciso V, da Lei de Diretrizes Orçamentárias (LDO) nº. 19.573, de 11 de agosto de 2011 e, quanto aos exercícios subseqüentes, pelas dotações próprias que forem fixadas nos respectivos orçamentos..



ANEXO II

TERMO DE CONFIDENCIALIDADE

PREGÃO ELETRÔNICO N.º 1191001 /2011

Processo nº. 0077447-1190-2010-4 – SIGED : 00011020-1191-2011

CELEBRANTE:

NOME: ESTADO DE MINAS GERAIS/SECRETARIA DE ESTADO DE FAZENDA

SEDE: Administrativa Tancredo Neves – Órgão: Secretaria de Estado de Fazenda – Prédio: Gerais – 6º andar - Rodovia Prefeito Américo Gianetti, s/nº, Bairro Serra Verde, no Município de Belo Horizonte/MG - CEP: 31630-901.

CNPJ: 18.715.615/0001-60

REPRESENTANTE LEGAL: Soraya Naffah Ferreira – Superintendente de Tecnologia e Informação

CELEBRADA:

NOME EMPRESARIAL:

ENDEREÇO:

CNPJ:

INSCRIÇÃO ESTADUAL:

REPRESENTANTE(S) LEGAL(is):

NOME:

CPF:

NOME:

CPF:

CONSIDERANDO que a **CELEBRADA** contratou com o **CELEBRANTE** a aquisição de solução de gerenciamento de identidades e de acessos, contemplando licenças de uso, *appliances* ou servidores, serviços de implantação, treinamento para capacitação de pessoal técnico da Superintendência de Tecnologia da Informação – STI/SEF, garantia dos *appliances* ou servidores e da ferramenta de gerenciamento de identidades e de acessos, originário do Pregão Eletrônico N° 1191001 - /2011;

CONSIDERANDO que para tanto a **CELEBRADA** receberá informações a respeito do negócio, sistemas e/ou equipamentos, sendo de natureza peculiar as atividades do **CELEBRANTE**,

RESOLVEM as partes firmar o presente Termo de Confidencialidade, que se regerá pelas cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA - DAS DEFINIÇÕES

I - Para os fins deste instrumento, entende-se por informação: os dados, os documentos e os materiais que lhe sejam pertinentes. A "informação" poderá se revestir da forma oral, escrita, ou qualquer outra, corpórea ou não, a exemplo de: fórmulas, algoritmos, processos, projetos, croquis, fotografias, plantas, desenhos, conceitos de produto, especificações, amostras de idéia, nomes de fornecedores, preços e custos, definições e informações de negócios.

II - É considerada informação sigilosa toda e qualquer informação ou dado fornecido, comunicado ou revelado à **CELEBRADA**, seja know-how e dados, seja de caráter técnico ou não, que esteja em



poder da **CELEBRANTE** e que seja revelado à **CELEBRADA** por necessidade de execução do trabalho contratado.

III - Toda a informação que a **CELEBRADA** tenha acesso ou que lhe seja fornecida pelo **CELEBRANTE**, será considerada sigilosa, salvo se estiver expressamente estipulado em contrário.

IV - Não será considerada sigilosa a:

- a) informação identificada como de domínio público;
- b) informação que se encontrava na posse legítima da **CELEBRADA**, livre de qualquer obrigação de sigilo, antes de sua revelação pelo **CELEBRANTE**;
- c) - informação expressamente identificada pelo **CELEBRANTE** como “não sigilosa”.

CLÁUSULA SEGUNDA – DAS OBRIGAÇÕES

As partes acordam:

a) não comercializar, divulgar, ceder, emprestar, revelar ou distribuir informação referente ao trabalho realizado, desde que autorizado pelo **CELEBRANTE**.

b) manter salvaguardas adequadas e seguras contra destruição, perda ou alteração dos arquivos de dados que o **CELEBRANTE** possa entregar à **CELEBRADA**, os quais ficarão sujeitos aos mesmos cuidados, proteção e segurança, dispensados àqueles da própria **CELEBRADA**, ficando esta livre e isenta de quaisquer responsabilidades em casos fortuitos ou de força maior;

c) respeitar e cumprir todas as estipulações referentes ao sigilo das informações;

d) devolver, independentemente de solicitação da outra parte, toda informação, sob qualquer forma que ela se encontre, bem como quaisquer cópias que eventualmente tenha em seu poder, após o término dos trabalhos sob contrato;

e) manter em absoluta segurança e devidamente protegidos todo e qualquer programa de computador, documentação correlata, material e/ou informação com dados sigilosos, ou que venham a ter conhecimento, obrigando-se, ainda, por si, seus funcionários ou agentes e usuários, a não divulgar e nem revelar a terceiros quaisquer informações, sem prévia autorização escrita.

CLÁUSULA TERCEIRA - DA IMPOSSIBILIDADE DE DIVULGAÇÃO DAS INFORMAÇÕES

Pelo presente Termo, a **CELEBRADA** reconhece a natureza sigilosa da informação que lhe será transmitida, sob forma escrita, oral, em meio magnético ou qualquer outra forma de acesso, pelo **CELEBRANTE** e compromete-se a:

a) manter sob absoluto sigilo todas as informações que lhe forem transmitidas, visando à execução dos trabalhos contratados;

b) responsabilizar-se integralmente pelos atos de seus empregados, praticados nas dependências do **CELEBRANTE**, ou mesmo fora delas, que venham a causar danos a esta ou a seus funcionários, com a substituição imediata daqueles que não corresponderem ao padrão de comportamento exigido;

d) permitir o acesso à informação apenas aos seus funcionários ou prepostos, que necessitem absolutamente de conhecê-la para os fins referidos, comunicando-lhes antecipadamente as obrigações assumidas em matéria de sigilo e impondo-lhes o seu cumprimento;

e) não utilizar informações do **CELEBRANTE** em benefício próprio ou de terceiros;

f) proteger as informações de divulgação a terceiros com o mesmo grau de cautela com que protege suas próprias informações de importância similar, tendo em vista a natureza dos negócios do **CELEBRANTE**;



- g) assegurar que, durante a execução dos serviços, seus empregados façam uso de crachás contendo o nome, a função e a denominação;
- h) credenciar junto ao **CELEBRANTE** todo o seu pessoal designado para a execução dos serviços, objeto deste Termo, sob pena de não lhe ser permitido o acesso às instalações;
- i) comunicar ao **CELEBRANTE** qualquer alteração relativa à titularidade ou gestão;
- j) instruir os encarregados, responsáveis pelo tratamento das informações confidenciais, a proteger e manter o sigilo das mesmas.

Parágrafo Primeiro

A **CELEBRADA**, para fins de sigilo, obriga-se por seus administradores, empregados e contratados.

Parágrafo Segundo

A obrigação de sigilo mantém-se, mesmo após o termo da vigência do contrato, só cessando após autorização escrita do **CELEBRANTE**.

CLÁUSULA QUARTA – DO DESCUMPRIMENTO

I - O não cumprimento do compromisso de sigilo, estabelecido neste instrumento, sujeitará a **CELEBRADA** ao pagamento das perdas e danos sofridos pelo **CELEBRANTE**, sem prejuízo das demais sanções legais cabíveis, decorrentes da violação deste Termo.

II - O não exercício pelas partes de qualquer direito a ela assegurado neste Termo, ou a não aplicação de qualquer medida, penalidade ou sanção possível, não importará em renúncia ou novação, não devendo, portanto, ser interpretada como desistência de sua aplicação em caso de reincidência.

CLÁUSULA QUINTA - DO DESEMPENHO DAS FUNÇÕES

I - O presente Termo obriga as partes e seus sucessores.

II - A Auditoria Setorial da Secretaria de Estado de Fazenda acompanhará e fiscalizará o cumprimento deste Termo.

III - Este Termo não poderá ser modificado, alterado ou rescindido, no todo ou em parte, exceto por documento escrito assinado entre as Partes.



CLÁUSULA SEXTA - DO FORO

As partes elegem o foro da Comarca de Belo Horizonte - MG para dirimir quaisquer dúvidas ou litígios eventualmente surgidos em decorrência deste instrumento.

E por estarem ajustadas, firmam este instrumento em 2 (duas) vias de igual teor e forma, na presença de duas testemunhas que também o assinam.

Belo Horizonte, de de 2011.

CELEBRANTE

CELEBRADA

TESTEMUNHAS:

1. _____
Nome:
CPF

2. _____
Nome:
CPF:



ANEXO III

MODELO DE PROPOSTA
PROPOSTA DE PREÇO/PLANILHA DE CUSTOS GLOBAL
PREGÃO ELETRÔNICO Nº 1191001 - /2011 - PROCESSO Nº 0077447-1190-2010-4

OBSERVAÇÕES:

1) PARA A COTAÇÃO DO VALOR GLOBAL, OS ITENS CONSTANTES DESTE ANEXO DEVERÃO SER OBSERVADOS POR TODOS OS FORNECEDORES.

2) SOMENTE O FORNECEDOR DETENTOR DA MELHOR PROPOSTA, DEVERÁ APRESENTAR ESTE ANEXO, APÓS A REALIZAÇÃO DA SESSÃO DESTE PREGÃO, CONFORME DISPOSTO NO SUBITEM 6.3.2 DESTE EDITAL.

3) O FORNECEDOR ESTABELECIDO NO ESTADO DE MINAS GERAIS, NO CASO DE DETENTOR DA MELHOR PROPOSTA, DEVERÁ ENCAMINHAR A PROPOSTA CONTENDO O PREÇO NORMAL DE MERCADO E O PREÇO RESULTANTE DA DEDUÇÃO DO ICMS, EXCETO O FORNECEDOR OPTANTE PELO SIMPLES NACIONAL, O QUAL DEVERÁ ENCAMINHAR A PROPOSTA PELO PREÇO OFERTADO, CONFORME DETERMINA A RESOLUÇÃO CONJUNTA SEPLAG/SEF Nº. 3.458, DE 22 DE JULHO DE 2003, QUE REGULAMENTA A ISENÇÃO DO ICMS PARA ESTE CASO.

4) O FORNECEDOR VENCEDOR DEVERÁ DECLARAR EXPRESSAMENTE QUE NOS PREÇOS COTADOS ENCONTRAM-SE INCLUSOS TODOS OS CUSTOS E DESPESAS PARA O FORNECIMENTO DA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADES E DE ACESSOS, TAIS COMO: CUSTOS DIRETOS E INDIRETOS, TRIBUTOS INCIDENTES, ENCARGOS SOCIAIS/ TRABALHISTAS, IMPOSTOS, TAXAS, SEGUROS, LUCRO, FRETE, CARGAS E DESCARGAS ATÉ O DESTINO, MATERIAIS, EQUIPAMENTOS, ACESSÓRIOS, SOFTWARES, *APPLIANCES* OU SERVIDORES, TREINAMENTOS, GARANTIA PELO PERÍODO DE 48 (QUARENTA E OITO) MESES E OUTRAS DESPESAS DE QUALQUER NATUREZA QUE SE FAÇAM INDISPENSÁVEIS À PLENA EXECUÇÃO DOS SERVIÇOS, OBJETO DA PRESENTE LICITAÇÃO.

PLANILHA DE CUSTOS		
LOTE ÚNICO		
SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADES E DE ACESSOS		
Descrição	Valor Unit. (R\$)	Valor Total (R\$)
Solução de gerenciamento de identidades e de acessos baseada em licenças de uso e <i>appliances</i> ou servidores (<i>software / hardware</i> (se houver) e respectivas licenças)		
Software		
Hardware		
Serviços de implantação da solução		
Serviços de treinamento para capacitação de pessoal técnico (aproximadamente 174 treinandos), indicado pela SEF-MG, na configuração, manutenção e uso das ferramentas envolvidas na solução.		
Garantia dos <i>appliances</i> ou servidores e da ferramenta de software para gerenciamento de identidades e de acessos, incluindo manutenção pelo prazo de 48 meses, bem como o fornecimento de novos releases e versões e suporte técnico na modalidade 24 X 7 pelo período de 48 meses.		
Horas de serviço de <i>coaching/mentoring</i>		
VALOR GLOBAL		R\$

NOME EMPRESARIAL:

CNPJ:

PRAZO DE VALIDADE DESTA PROPOSTA: 60 dias.

DATA:



ASSINATURA E CARIMBO DO REPRESENTANTE LEGAL:

ANEXO IV

PREGÃO ELETRÔNICO N.º 1191001 /2011

Processo n.º 0077447-1190-2010-4

MINUTA DO CONTRATO

CONTRATO PARA AQUISIÇÃO DE UMA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADES E DE ACESSOS DA SECRETARIA DE ESTADO DE FAZENDA DE MINAS GERAIS, ORIGINÁRIO DA LICITAÇÃO NA MODALIDADE DE PREGÃO ELETRÔNICO N.º 1191001 -/2011, TIPO MENOR PREÇO, PROCESSO N.º 0077447-1190-2010-4, REGIDO PELA LEI FEDERAL N.º 8.666, DE 21 DE JUNHO DE 1993, E PELAS CONDIÇÕES ESTABELECIDAS NO PRESENTE CONTRATO, OBSERVADOS OS PRECEITOS DA LEI ESTADUAL N.º 13.994, DE 18 DE SETEMBRO DE 2001, E DO DECRETO ESTADUAL N.º 44.431, DE 29 DE DEZEMBRO DE 2006.

CONTRATANTE

CONTRATANTE: ESTADO DE MINAS GERAIS/SECRETARIA DE ESTADO DE FAZENDA/SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

ENDEREÇO: Cidade Administrativa - Rodovia Prefeito Américo Gianetti, s/nº, Prédio Gerais - 6º Andar, Bairro Serra Verde - Belo Horizonte/MG- CEP:31630-901

CNPJ/MF: 18.715.615/0001-60

REPRESENTANTE LEGAL: Soraya Naffah Ferreira, Superintendente de Tecnologia e Informação, credenciada na forma do Ato do Secretário Estadual de Fazenda n.º 3.960, de 12/02/2008.

CONTRATADO

NOME EMPRESARIAL:

ENDEREÇO:

CNPJ/MF:

INSCRIÇÃO ESTADUAL:

REPRESENTANTE LEGAL:

CI (RG) : _____ CPF: _____

CLÁUSULA PRIMEIRA - DO OBJETO

Constitui objeto desta licitação a aquisição de uma solução de gerenciamento de identidades e de acessos, contemplando licenças de uso, *appliances* ou servidores, serviços de implantação, treinamento para capacitação de pessoal técnico da Superintendência de Tecnologia da Informação – STI/SEF, garantia dos *appliances* ou servidores e da ferramenta de gerenciamento de identidades e de acessos, como solução de provisionamento de usuários para os sistemas da SEF/MG, de acordo com as especificações e demais condições previstas no Anexo I (Termo de Referência), parte integrante deste instrumento.



CLÁUSULA SEGUNDA – DO LOCAL DA ENTREGA E DA FORMA DE RECEBIMENTO

LOTE ÚNICO			
AQUISIÇÃO DE SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADES E DE ACESSOS			
Item	Descrição	Quant.	Prazo de Entrega
1	Fornecimento de hardware (<i>appliance</i> s ou servidores) para compor a solução de gerenciamento de identidades e de acessos.	1	90 (noventa) dias contados da assinatura do contrato.
2	Fornecimento de software (licenças de uso) para compor a solução de gerenciamento de identidades e de acessos baseada	1	90 (noventa) dias contados da assinatura do contrato.
3	Serviços de implantação da solução	1	240 (duzentos e quarenta) dias contados da assinatura do contrato.
4	Serviços de treinamento para capacitação de pessoal técnico (aproximadamente 174 treinandos), indicado pela SEF-MG, na configuração, manutenção e uso das ferramentas envolvidas na solução.	1	300 (trezentos) dias contados da assinatura do contrato.
5	Garantia dos <i>appliance</i> s ou servidores e da ferramenta de software para gerenciamento de identidades e de acessos, incluindo manutenção pelo prazo de 48 meses, bem como o fornecimento de novos releases e versões e suporte técnico na modalidade 24 horas por dia X 7 dias por semana, pelo período de 48 meses.	1	Imediatamente após a expedição do Termo de Recebimento referente aos itens 1, 2, condicionada à instalação e configuração preliminar desses componentes da solução, que deverá ocorrer até 120 (cento e vinte) dias após a assinatura do contrato.
6	Horas de serviço de <i>coaching/mentoring</i>	1000	Sob demanda, podendo ser executado durante 12 (doze) meses após a assinatura do contrato

I - O **CONTRATADO**, de posse da requisição e da nota fiscal respectiva, deverá entregar os softwares objetos deste contrato, na Superintendência de Tecnologia da Informação da Secretaria de Estado de Fazenda, situada na rua Alagoas, 880 – Funcionários – Belo Horizonte – MG, de acordo com as especificações técnicas do Anexo I do edital, parte integrante deste instrumento contratual.

II – O recebimento do objeto deste contrato deverá ser realizado perante servidor credenciado pela **CONTRATANTE**, de acordo com os critérios de aceitabilidade estabelecidos no item 2 do Anexo I – Termo de Referência e conforme a seguir:

- a) **provisoriamente**: de posse da proposta respectiva, serão recebidos os produtos/serviços para verificação de especificações, qualidade, prazos, preços, e outros dados pertinentes



e, encontrada alguma irregularidade, será fixado prazo para sua correção, ou se aprovado, receberá o objeto deste contrato, mediante recibo;

- b) **definitivamente:** após recebimento provisório, será realizada a conferência dos produtos e serviços, e estando de acordo com a requisição emitida pelo **CONTRATANTE**, e com as exigências contratuais, inclusive de instalação e configuração preliminar do hardware e do software fornecidos, será efetivado o recebimento definitivo, mediante expedição de Termo de Recebimento aposto nas vias da nota fiscal, ou no documento auxiliar da NF-e (Danfe).

III – Na hipótese de os produtos/serviços apresentarem irregularidades não sanadas, será reduzido a termo o fato e encaminhado à autoridade competente, para procedimentos inerentes à aplicação das penalidades.

IV - Serão expedidos Termos de Aceite Técnico, pela Superintendência de Tecnologia da Informação – STI, na forma prevista no item 2 do Anexo I, para:

- a solução de hardware e software fornecida, envolvendo testes de funcionamento e verificação do cumprimento dos requisitos previstos na especificação técnica além de realização de todas as atividades de instalação, configuração ;
- garantia, envolvendo verificação da disponibilidade de suporte técnico para o hardware e software fornecidos;
- coaching/mentoring, atestando, mensalmente, as atividades demandas pela SEF e executadas satisfatoriamente no mês anterior;
- treinamento, mediante verificação da conclusão satisfatória do treinamento e expedição dos certificados para os treinandos com 75% de presença.

V - O recebimento e o aceite técnico definitivos não eximirão o **CONTRATADO** de suas responsabilidades, nem invalidarão ou comprometerão qualquer reclamação que o **CONTRATANTE** venha a fazer, baseada na existência de produto inadequado ou defeituoso, no prazo da garantia.

CLÁUSULA TERCEIRA - DO PRAZO

Este contrato terá vigência pelo prazo de 52 (cinquenta e dois) meses, a contar da data de sua assinatura.

CLÁUSULA QUARTA - DO PREÇO

I - Os valores a serem pagos ao **CONTRATADO** será de R\$ _____ (_____), conforme especificado a seguir:

PLANILHA DE CUSTOS		
LOTE ÚNICO		
SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADES E DE ACESSOS		
Descrição	Valor Unit. (R\$)	Valor Total (R\$)
Solução de gerenciamento de identidades e de acessos baseada em licenças de uso e <i>appliances</i> ou servidores (software / hardware (se houver) e respectivas licenças)		
Software		
Hardware		
Serviços de implantação da solução		
Serviços de treinamento para capacitação de pessoal técnico (aproximadamente 174 treinandos), indicado pela SEF-MG, na configuração, manutenção e uso das ferramentas envolvidas na solução.		
Garantia dos <i>appliances</i> ou servidores e da ferramenta de software para gerenciamento de identidades e de acessos,		



incluindo manutenção pelo prazo de 48 meses, bem como o fornecimento de novos releases e versões e suporte técnico na modalidade 24 X 7 pelo período de 48 meses.		
Horas de serviço de <i>coaching/mentoring</i>		
VALOR GLOBAL		R\$

II - No preço estabelecido nesta cláusula estão incluídos todos os custos e despesas, tais como: custos diretos e indiretos, tributos incidentes, encargos sociais/trabalhistas, impostos, taxas, seguros, lucro, frete, cargas e descargas até o destino, materiais, equipamentos, inclusive *appliances* ou servidores, acessórios, softwares, treinamentos, garantia pelo período de 48 (quarenta e oito) meses e outras despesas de qualquer natureza que se façam indispensáveis à plena execução dos serviços, objeto do presente contrato.

CLÁUSULA QUINTA - DO PAGAMENTO

I - O **CONTRATADO** deverá emitir os documentos fiscais, em valores unitário e global, com os seguintes dados:

a) Dados do CONTRATANTE:

Nome: ESTADO DE MINAS GERAIS/SECRETARIA DE ESTADO DE FAZENDA
CNPJ: 18.715.615/0001-60
Endereço: Cidade Administrativa – Rodovia Prefeito Américo Gianetti s/nº – Prédio Gerais – 6º Andar - Bairro Serra Verde – Belo Horizonte/MG – CEP: 31630-901.

b) Dados do CONTRATADO:

Banco: _____
Agência: _____
Número da conta: _____

II - O pagamento de cada etapa será efetuado através do Sistema Integrado de Administração Financeira - SIAFI/MG, por meio de crédito em conta bancária do **CONTRATADO**, cumprida a etapa de acordo com o cronograma físico-financeiro apresentado a seguir, no prazo de até 30 (trintas) dias, contados após a emissão dos Termo de Recebimento ou do Termo de Aceite Técnico pela Superintendência de Tecnologia da Informação – STI/SEF, **respeitado o cronograma físico-financeiro** abaixo, com base na(s) Nota(s) Fiscal(is) ou Documento Auxiliar de Nota Fiscal eletrônica (NF-e) - Danfe, devidamente conferido(s) e atestado(s) por responsável pelo recebimento, sendo que o atraso na entrega dos documentos de cobrança implicará a prorrogação do vencimento, proporcionalmente aos dias de atraso.

III – O pagamento se dará em parcelas, conforme detalhado no quadro a seguir, e após ser verificado o cumprimento das atividades previstas no cronograma de entrega dos produtos/serviços abaixo, levando-se em conta a efetiva entrega dos produtos e prestação dos serviços:

CRONOGRAMA DE DESEMBOLSO FÍSICO-FINANCEIRO

CRONOGRAMA FÍSICO-FINANCEIRO		
Item	Descrição	Pagamento
1	<i>Appliances</i> ou servidores (hardware) que compõem a solução de gerenciamento de identidades e de acessos	12% do somatório dos valores correspondentes ao hardware, software e implantação da solução, excluindo-se para apuração desse total os valores correspondentes a treinamento e <i>coaching/mentoring</i> , a serem pagos após recebimento do



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

		hardware, mediante expedição de Termo de Recebimento pela Superintendência de Tecnologia da Informação/SEF.
2	Licenças de uso de software que compõem a solução de gerenciamento de identidades e de acessos	48% do somatório dos valores correspondentes ao hardware, software e implantação da solução, excluindo-se para apuração desse total os valores correspondentes a treinamento e coaching/mentoring, a serem pagos após recebimento dos certificados de licença, mídias, manuais do software, mediante expedição de Termo de Recebimento pela Superintendência de Tecnologia da Informação/SEF.
3	Implantação da solução	30% do somatório dos valores correspondentes ao hardware, software e implantação da solução, excluindo-se para apuração desse total os valores correspondentes a treinamento e <i>coaching/mentoring</i> , a serem pagos depois de cumpridas as exigências previstas no subitem 1.2.2 do Anexo I - Termo de Referência. Será realizada a expedição de Termo de Aceite Técnico pela Superintendência de Tecnologia da Informação/SEF para comprovar a realização da etapa de implantação da solução.
4	Treinamento	Valor total cotado para o treinamento, a ser pago após a realização satisfatória dos treinamentos, da emissão de certificado de conclusão do treinamento e da expedição do Termo de Aceite Técnico referente ao treinamento.
5	Garantia dos <i>appliances</i> ou servidores e da ferramenta de software para gerenciamento de identidades e de acessos	10% do somatório dos valores correspondentes ao hardware, software e implantação da solução, excluindo-se para apuração desse total os valores correspondentes a treinamento e <i>coaching/mentoring</i> , a serem pagos após a expedição de Termo de Aceite Técnico referente à garantia pela Superintendência de Tecnologia da Informação/SEF.
6	Horas de <i>coaching/mentoring</i>	Pagamento mensal após a conclusão satisfatória dos serviços contratados e desenvolvidos no mês anterior, devidamente comprovada mediante expedição do Termo de Aceite Técnico referente ao <i>coaching/mentoring</i>

IV – Após o recebimento definitivo dos produtos/serviços pelo servidor credenciado, a(s) Nota(s) Fiscal(is)/Fatura(s) deverão ser remetidas à Secretaria de Estado de Fazenda/Superintendência de Tecnologia e Informação, Cidade Administrativa – Rodovia Prefeito Américo Gianetti s/nº – Prédio



Gerais – 6º Andar – Lado ímpar -Bairro Serra Verde – Belo Horizonte – MG – CEP: 31630-901, para fins de pagamento.

V - As Notas Fiscais que apresentarem incorreções serão devolvidas ao **CONTRATADO** para as devidas correções e o prazo para o pagamento passará a correr a partir da data da reapresentação do documento, considerado válido pelo **CONTRATANTE**.

VI - No caso de providências complementares por parte do **CONTRATADO**, o prazo para pagamento será interrompido, reiniciando-se sua contagem a partir da data em que houver o cumprimento definitivo da ocorrência, não sendo devida nesses casos atualização financeira.

VI - Ocorrendo atraso de pagamento por culpa exclusiva do **CONTRATANTE**, o valor devido será atualizado financeiramente, entre as datas do vencimento e do efetivo pagamento, de acordo com a variação “*pro-rata tempore*” do IPCA.

CLÁUSULA SEXTA - DO REAJUSTAMENTO

Os valores a que se refere à Cláusula Quarta não poderão ser reajustados durante a vigência deste contrato.

CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DAS PARTES

I – DO CONTRATADO

a) manter as condições de habilitação e qualificações exigidas no ato convocatório, responsabilizando-se pelo fornecimento, podendo, na hipótese de serviços de instalação de infraestrutura de rede lógica e elétrica, ceder ou subcontratar, total ou parcialmente o objeto deste contrato;

b) entregar os bens, na quantidade, qualidade, local e prazos especificados neste Contrato e seus respectivos anexos, apresentando documento garantindo o suporte no Brasil em português, 24 horas por dia, 7 dias por semana;

c) entregar os serviços de acordo com as especificações constantes do Anexo I (Termo de Referência), dentro do prazo estabelecido neste Contrato e nos termos da legislação vigente;

d) prestar, sem quaisquer ônus para o **CONTRATANTE**, os serviços necessários à correção e revisão de falhas ou defeitos verificados no trabalho, sempre que a ela imputáveis;

e) estabelecer, em conjunto com o **CONTRATANTE**, cronograma para a execução dos serviços;

f) responsabilizar-se pelos danos causados ao **CONTRATANTE** ou a terceiros, decorrentes de sua culpa ou dolo, não excluindo ou reduzindo essa responsabilidade à fiscalização deficiente por parte do **CONTRATANTE**;

g) firmar Termo de Confidencialidade, que integrará este Contrato, conforme modelo do Anexo II, no qual se compromete a não divulgar, sem autorização, quaisquer informações do **CONTRATANTE**, a que tiver conhecimento em razão da execução deste Contrato;

h) durante a vigência do contrato, fornecer todas as atualizações do software que é objeto desta contratação, sem necessidade de qualquer solicitação ou notificação;

i) prestar assistência técnica e manutenção, durante o período de garantia, de acordo com os manuais e normas técnicas específicos, a fim de manter os equipamentos e softwares em perfeitas condições de uso, independentemente do defeito a ser detectado, incluindo mão-de-obra, substituição de peças/componentes, reparos necessários, atualização e suporte técnico dos softwares e demais custos decorrentes do serviço a ser executado, sem ônus para o **CONTRATANTE**;



- j) reparar, corrigir, remover, refazer, reconstituir ou substituir total ou parcialmente, às suas expensas, os serviços ou materiais empregados, objeto deste contrato, em que se verifiquem vício, defeito ou incorreção resultante da execução irregular ou inadequada, no prazo máximo de 10 (dez) dias úteis, contados da data da notificação expedida pelo **CONTRATANTE**, visando o atendimento das especificações, sem prejuízos da aplicação das sanções previstas;
- k) sujeitar-se à fiscalização do **CONTRATANTE**, por meio de servidor por ela credenciado, ou por técnico especializado, quando for necessária a vistoria, para comprovação da perfeita execução dos serviços;
- l) responsabilizar-se pelo exato cumprimento de todas as obrigações e exigências decorrentes da legislação trabalhista e previdenciária, ficando claro inexistir entre seus empregados e o **CONTRATANTE** vínculo empregatício ou de qualquer outra natureza, razão pela qual correrão por conta exclusiva do **CONTRATADO** todos os ônus decorrentes de rescisões de contratos de trabalho e atos de subordinação de seu pessoal;
- m) responsabilizar-se integralmente pelos serviços contratados, assumindo inteira responsabilidade técnica e administrativa do objeto, não podendo, sob qualquer hipótese, transferir a outras empresas a responsabilidade por problemas de funcionamento do serviço;
- n) fornecer aos técnicos designados para executarem os serviços, obrigatoriamente, crachás de identificação, contendo nome, função e denominação da empresa em que trabalham para acesso às dependências do **CONTRATANTE**;
- o) responsabilizar-se pelo recolhimento de impostos sobre os serviços prestados e, se for o caso, sobre os bens fornecidos;
- p) fornecer e manter atualizado o nome completo, telefone e endereço de correio eletrônico do gerente responsável pelo acompanhamento dos serviços contratados;
- q) responsabilizar-se pelos ônus relativos ao fornecimento dos equipamentos/materiais, inclusive fretes e seguros, desde a origem até sua entrega no local de destino;
- r) ministrar treinamento para o corpo técnico do **CONTRATANTE**, após a implantação da solução ofertada;
- s) conceder garantia para o objeto contratual, pelo prazo de 48 (quarenta e oito) meses, contados a partir do momento do aceite técnico do **CONTRATANTE**;
- t) cumprir e respeitar as normas vigentes da Política de Segurança da Informação do **CONTRATANTE**;
- u) apresentar à STI/SEF, para aprovação, no prazo máximo de 10 (dez) dias úteis após assinatura do Contrato, plano de trabalho acompanhado de cronograma para a execução dos serviços;
- v) emitir documentos fiscais referentes à prestação dos serviços.
- z) prestar, sempre que demandado pelo **CONTRATANTE**, serviços de coaching/mentoring, na forma prevista no Anexo I – Termo de Referência do Edital que resultou nesta contratação.

II – DO CONTRATANTE

- a) elaborar juntamente com o **CONTRATADO**, cronograma de atividades para a execução dos serviços;
- b) promover, por intermédio de servidor designado, o acompanhamento e a fiscalização da prestação dos serviços, rejeitando aqueles que não atenderem a qualidade exigida, anotando em registro próprio as falhas detectadas e exigindo medidas corretivas por parte do **CONTRATADO**;
- c) notificar o **CONTRATADO**, fixando-lhe prazo para corrigir irregularidades encontradas na



execução dos serviços;

d) acompanhar, monitorar e avaliar os resultados dos serviços executados, visando garantir a qualidade dos serviços contratados;

e) promover o recebimento provisório e o definitivo dos bens e softwares e a aceitação técnica dos bens, softwares e demais serviços;

f) assegurar ao pessoal do **CONTRATADO** amplo e livre acesso às instalações para a plena execução do contrato, observadas as normas de segurança e horário de funcionamento do **CONTRATANTE**;

g) instruir seus servidores e prepostos a respeito das disposições deste contrato;

h) fornecer ao **CONTRATADO**, em tempo hábil, toda informação e documentação técnica de que dispõe e que sejam, a seu critério, consideradas necessárias à execução dos serviços;

i) colaborar com o **CONTRATADO**, quando solicitado, facilitando-lhe o cumprimento dos serviços ora contratados;

j) disponibilizar, durante o período de trabalho a ser realizado nas dependências do **CONTRATANTE**, uma equipe funcional e técnica, capacitada a atender aos requisitos da contratação, inclusive a nível gerencial e decisório;

k) emitir o Termo de Aceite Técnico, após conclusão de cada uma das etapas de serviços descrita no cronograma físico-financeiro, desde que o serviço tenha sido realizado em conformidade com o escopo contratado e de acordo com todos requisitos previstos neste contrato;

l) aprovar as etapas de execução dos serviços, previstas no cronograma apresentado pelo **CONTRATADO**, desde o planejamento até a sua efetiva concretização;

m) fornecer *feedback* sobre os serviços, ao **CONTRATADO**, regularmente;

n) fornecer espaço adequado, telefone, acesso à Internet de alta velocidade e acesso a seus sistemas internos, além das ferramentas necessárias para o **CONTRATADO** executar os serviços;

o) efetuar o pagamento pela execução do objeto contratual.

CLÁUSULA OITAVA - DAS ALTERAÇÕES

O presente contrato poderá ser alterado nos casos previstos no artigo 65 da Lei nº. 8.666/93, desde que devidamente fundamentado e autorizado pela autoridade superior.

CLÁUSULA NONA - DO VALOR ESTIMADO

Para efeitos legais, estima-se o valor total deste Contrato em R\$ _____
(_____).

CLÁUSULA DÉCIMA - DA DOTAÇÃO ORÇAMENTÁRIA

As despesas decorrentes da contratação correrão por conta das dotações orçamentárias n.ºs. 1191.04.129.029.1248.0001.3390.39, fonte 10 e/ou 25.1 e/ou 1191.04.129.029.1248.0001.4490.52., fonte 10.1 e ou 25.1, consignadas na Lei Orçamentária Anual (LOA) que for aprovada para o exercício de 2012, ou no Projeto de Lei Orçamentária Anual (PLOA) 2521/2011, publicado no Diário do Legislativo em 06 de outubro de 2011, encaminhado pela Mensagem do Governador nº 125/2011, de 29 de setembro de 2011, caso este não seja sancionado até o dia 31 de dezembro de 2011, conforme autorizado pelo art. 53, inciso V, da Lei de Diretrizes Orçamentárias (LDO) nº.



19.573, de 11 de agosto de 2011 e, quanto aos exercícios subseqüentes, pelas dotações próprias que forem fixadas nos respectivos orçamentos.

CLÁUSULA DÉCIMA PRIMEIRA - DAS PENALIDADES

Pela inexecução total ou parcial do contrato ou por fraudar a execução deste, a Administração poderá, garantida a prévia defesa, aplicar ao **CONTRATADO** as seguintes sanções:

I - advertência escrita - comunicação formal quanto à conduta do **CONTRATADO** sobre o descumprimento do contrato e outras obrigações assumidas, e a determinação da adoção das necessárias medidas de correção.

II – multa, a qual deverá observar os seguintes limites máximos:

a) 0,3% (três décimos por cento) por dia, até o trigésimo dia de atraso, sobre o valor do serviço ou fornecimento não realizado ou por atraso no atendimento de chamado de suporte técnico, neste caso sendo considerado o dia ou fração;

b) 2% (dois por cento) sobre o valor total do contrato, em caso de descumprimento das demais obrigações contratuais ou norma da legislação pertinente;

c) 20% (vinte por cento) sobre o valor do serviço ou fornecimento não realizado, no caso de atraso superior a 30 (trinta) dias, inclusive para atraso no atendimento de chamado de suporte técnico, ou entrega do objeto com vícios ou defeitos ocultos que o torne impróprio ao uso a que é destinado, ou diminua-lhe o valor ou, ainda, fora das especificações contratadas;

III - suspensão temporária de participação em licitação e impedimento de contratar com a Administração Pública Estadual, por prazo não superior a 02 (dois) anos, nos termos do inciso III, do artigo 87 da Lei nº. 8.666/93.

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 do **CONTRATADO** perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o **CONTRATADO** ressarcir a Administração Pública Estadual pelos prejuízos resultantes de ação ou omissão do mesmo, nos termos do artigo 34, II, do Decreto nº. 44.431, de 29 de dezembro de 2006.

PARÁGRAFO ÚNICO

I - As penalidades de advertência e multa serão aplicadas de ofício ou por provocação dos órgãos de controle, pela autoridade signatária deste contrato.

II - As sanções previstas nos incisos I, III e IV poderão ser aplicadas cumulativamente à prevista no inciso II, assegurado o direito de defesa prévia do **CONTRATADO** no prazo de 5 (cinco) dias úteis.

III – O valor da multa prevista no inciso II, desta Cláusula, será cobrado judicialmente ou retido dos pagamentos devidos pela Administração Pública Estadual, nos termos do § 1º do art. 18 do Decreto 44.431/2009.

IV - As penalidades contidas nesta Cláusula não impedem a rescisão unilateral do Contrato.

V – Nenhuma parte será responsável perante a outra pelos atrasos ocasionados por motivo de força maior ou caso fortuito.

VI – Poderão ser suspensas as penalidades, no todo ou em parte, quando o atraso na entrega dos serviços for devidamente justificado pelo **CONTRATADO** e desde que aceito pelo **CONTRATANTE**, que fixará novo prazo, este improrrogável, visando cumprir as obrigações contratuais.



CLAÚSULA DÉCIMA SEGUNDA – DA RESCISÃO

De acordo com o art. 79 da Lei nº. 8.666/93, a rescisão do contrato poderá ser:

I - por ato unilateral e escrito da Administração nos casos enumerados nos incisos I a XII e XVII do artigo 78 da citada Lei;

II - amigável, por acordo entre as partes, reduzido a termo no processo respectivo, desde que haja conveniência para a Administração;

III - judicial, nos termos da legislação.

PARÁGRAFO ÚNICO

No caso da rescisão unilateral, o **CONTRATANTE** não indenizará ao **CONTRATADO**, salvo pelos serviços prestados e aceitos definitivamente.

CLÁUSULA DÉCIMA TERCEIRA - DA FISCALIZAÇÃO

Compete à Diretoria de Infraestrutura e Operações-DIO/Superintendência de Tecnologia da Informação – STI/SEF fiscalizar, acompanhar a execução contratual, bem como, fazer cumprir as cláusulas e condições descritas neste Contrato.

CLÁUSULA DÉCIMA QUARTA – DAS DISPOSIÇÕES GERAIS

I - Todos os avisos e comunicações previstos neste instrumento deverão ser feitos por escrito.

II - O disposto neste contrato somente poderá ser alterado pelas partes por meio de termos aditivos ou quando a lei o permitir, por simples apostila.

III - É vedada a contratação de servidores do **CONTRATANTE** para prestarem quaisquer serviços, objeto deste Contrato.

IV - É permitido ao **CONTRATADO** a subcontratação parcial somente dos serviços de infraestrutura de rede lógica e elétrica, desde que submetida e expressamente autorizada pela Superintendência de Planejamento e Informática – STI/SEF.

CLÁUSULA DÉCIMA QUINTA - DA PUBLICAÇÃO

O **CONTRATANTE** providenciará a publicação do extrato do contrato na Imprensa Oficial de Minas Gerais, em obediência ao disposto no parágrafo único do art. 61 da Lei Federal nº 8.666/1993.

CLÁUSULA DÉCIMA SEXTA - DO FORO

As partes elegem o foro da Comarca de Belo Horizonte/MG para dirimir quaisquer dúvidas ou litígios decorrentes deste Contrato.

E por estarem ajustadas, firmam este instrumento em 02 (duas) vias, de igual teor, juntamente com as testemunhas que também o assinam.

Belo Horizonte, _____ de _____ de 2011.



ESTADO DE MINAS GERAIS
SECRETARIA DE ESTADO DE FAZENDA
SUPERINTENDÊNCIA DE GESTÃO E FINANÇAS

CONTRATANTE

ESTADO DE MINAS GERAIS/SECRETARIA DE ESTADO DE FAZENDA

CONTRATADO

NOME EMPRESARIAL DO FORNECEDOR

TESTEMUNHAS

1) _____
Nome:
CPF/MF:

2) _____
Nome:
CPF/MF: