



ATA DE CONSULTA PÚBLICA

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

Aos 26 dias do mês de outubro de 2011, reuniram-se em sessão de Consulta Pública, na sala de reunião do 7º andar do prédio Gerais, da Cidade Administrativa, localizado na Rodovia Prefeito Américo Gianetti, nº 4001, Bairro Serra Verde, em Belo Horizonte/MG, as servidoras Marília Izabel de Almeida e Eliana Mara Marcolino, representantes da Diretoria de Compras/SGF/SEF/MG; Lindenberg Naffah Ferreira, representante do gabinete do Secretário Adjunto (Assessoria), Rogério Zupo Braga, Flávio Damiance Ferreira e Alex Discacciati Neves, representantes da Superintendência de Tecnologia da Informação/STI/SEF/MG; Leonardo de Castro Myrrha, representante da Assessoria Jurídica/AJ/SEF/MG; Kassius C. de Vasconcelos e José Humberto Cruvinel, representantes da PRODEMGE; Thiago do Espírito Santo, representante da empresa Interadapt; Leandro Turbino e Hugo Higashi, representantes da empresa Novell; Janssen Lobo, representante da empresa IBM; Paulo Marques de Azevedo, representante da empresa Accenture, Luciano Azevedo de Souza, representante da empresa Safe e Alessandro Camargo Pereira, representante da empresa Nexa.

A sessão foi iniciada pela representante da SGF, Eliana Mara Marcolino, momento em que o edital em questão foi projetado e o representante do gabinete do Secretário Adjunto, Lindenberg Naffah Ferreira, fez uma breve explanação do que se pretende com a contratação. A seguir a sessão foi aberta para esclarecimentos de dúvidas e sugestões.

Foram apresentados pela empresa IBM os seguintes apontamentos:

1 – No Termo de Referência (Anexo I), subitem 1.2.1, inciso XXXV – “A solução deve ter a capacidade de permitir o auto-registro de usuários baseado em políticas de autorização e regras de negócio associadas”.

Sugerido: “A solução deve ter a capacidade de permitir o auto-registro de usuários baseado em políticas de autorização e regras de negócio associadas, **sendo permitido customizar de forma nativa (funcionalidade nativa customizada)**”.

Definido: A redação será alterada.

2 – No Termo de Referência (Anexo I), subitem 1.2.1, inciso 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)”:

j) “A solução deve ter mecanismo nativo que bloqueie **ou exclua acessos**, a partir de regras estabelecidas”.

Sugerido: “j) A solução deve ter mecanismo nativo que bloqueie acessos, a partir de regras estabelecidas”.

Definido: A redação original não é restritiva. A própria empresa que apresentou o questionamento atende a exigência constante deste item com a solução que ela fabrica. Assim sendo, a redação original será mantida.

3 – No Termo de Referência (Anexo I), subitem 1.2.1, inciso 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”.

Sugerido: Não é possível gerar o código de reativação sem que seja respondida uma pergunta desafio, no caso da solução fornecida pela IBM.



Definido: A redação será alterada, conforme sugestão da PRODEMGE, da seguinte maneira: “LXXVII. A solução deve possuir funcionalidade para tratamento de situações de esquecimento de senhas por usuários, através de pergunta de desafio, com a possibilidade de geração de um código de reativação (com prazo de expiração)”.

4 – No Termo de Referência (Anexo I), subitem 1.2.1, inciso – LXXXI – “A solução deve impedir o logon simultâneo em máquinas diferentes”.

Sugerido: “LXXXI. Para aplicações integradas à solução de gestão de identidade e acesso, a solução deve impedir o logon simultâneo em máquinas diferentes.”

Definido: A redação será alterada.

5 – No Termo de Referência (Anexo I), subitem 1.2.1, inciso – XC. f.- “Descrição: Deverão ser estabelecidos padrões de uso do sistema para cada grupo de usuários e, caso haja incoerência ou desvio, deverá ser realizado registro. (Ex: poderá possuir um padrão de acesso baseado em horário, duração e frequência). Mecanismos necessários para implementação: 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.”

Sugerido: Inicialmente, foi sugerida a exclusão do inciso XC. f.-do subitem 1.2.1, já que a definição de padrões não é responsabilidade da ferramenta, e sim dos gestores da SEF. Após discussão do assunto, concluiu-se pela necessidade de alteração da redação, da forma abaixo, a fim de proporcionar maior clareza em relação ao que estava sendo exigido.

Descrição:

A solução deverá permitir a configuração de atributos de uso de sistema, tais como horários, duração e frequência, para grupos de usuários e, caso haja desvios, deverá ser realizado registro. Mecanismos necessários para implementação:

A solução deverá permitir que todo usuário seja associado a um perfil de acesso. Deverá permitir, ainda, a configuração dos atributos de uso do sistema, tais como horários, duração, e frequência para esses perfis de acesso. Caso haja incoerência ou desvio, deverá ser realizado um registro.

Definido: A redação será alterada

6 – No Termo de Referência (Anexo I), subitem 1.2.1, inciso – XC. ap – “Descrição: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. Mecanismos necessários para implementação: Após a segunda falha de autenticação com a mesma credencial, o usuário deverá ser encaminhado para sistema de recuperação de credenciais.”

Sugerido: O representante da IBM informou que a solução fabricada/desenvolvida por essa empresa não permite redirecionar o usuário automaticamente para sistema de recuperação de credenciais. Assim sendo, foi proposta adequação na redação, da forma descrita em seguida.

Descrição:

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, deverá ser exibida uma mensagem informando um link para o sistema de recuperação de credenciais ou deverá ser efetuado o redirecionamento automático para o sistema de recuperação de credenciais.

Mecanismos necessários para implementação:

Após a segunda falha de autenticação com a mesma credencial, deverá ser exibida uma mensagem informando um link para o sistema de recuperação de credenciais ou deverá ser efetuado o redirecionamento automático para o sistema de recuperação de credenciais.

Definido: A redação será alterada.

7 – No Termo de Referência (Anexo I), subitem 1.2.1, inciso – XC ar - “Descrição: 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. Mecanismos necessários para implementação: 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.”

Sugerido: Exclusão do subitem “ar”, item XC.

Definido: A redação será alterada, retirando-se a exigência de bloqueio por 15 minutos, da forma descrita a seguir.

Descrição:

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 para o sistema ou computador de origem.

Mecanismos necessários para implementação:

Após a quinta tentativa de acesso sem sucesso, independente da credencial utilizada, o acesso ao sistema deverá ser bloqueado para o sistema/ computador de origem.

8 - No Termo de Referência (Anexo I), subitem 1.2.15, inciso 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.

Sugerido: Que a exigência da **declaração do fabricante** passe a ser feita na habilitação.

Definido: A SEF comprometeu-se no momento da sessão de consulta pública, a avaliar os aspectos jurídicos da sugestão apresentada. Feita essa análise, concluiu pela conveniência de exigir, para fins de habilitação, declaração do próprio licitante informando que é credenciado pelo fabricante, para comercializar, prestar e garantir serviços (ou fornecer e garantir os produtos) objeto da licitação, sob pena de rescisão unilateral do contrato pela SEF/MG e da aplicação das sanções legais cabíveis, sem prejuízos das perdas e danos. A exigência de declaração do licitante tem amparo na maioria dos julgados do Tribunal de Contas da União – TCU, o que não ocorre com a declaração do fabricante sugerida. Além disso, permite que a SEF requisite, durante a execução do contrato, comprovação de credenciamento do licitante vencedor do certame, mediante documento emitido pelo fabricante, se e quando entender necessário, podendo aplicar as penalidades cabíveis e, inclusive, rescindir o contrato, caso se constate falsa a declaração.

9 - No contrato (Anexo IV), cláusula quinta, “Cronograma de Desembolso Físico-Financeiro”.

Sugerido: O parcelamento do pagamento do valor correspondente ao software pode penalizar tanto o fornecedor quanto o fabricante. Sugere alterar a redação, pedindo para que o fornecedor abra a planilha de custos.

Definido: A redação será alterada. O pagamento dos softwares e do hardware será feito integralmente após o seu recebimento, com o pagamento dos serviços de implantação condicionado à sua aceitação. A planilha de custos passará a ter a composição abaixo.

PLANILHA DE CUSTOS			
LOTE ÚNICO			
SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADES E DE ACESSOS			
Descrição	Valor Unit. (R\$)	Quantidade	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			
Licença do software 1 que integra a solução, com nome completo do produto, devendo ser informados sua			



versão, <i>release</i> e modalidade de licenciamento (usuário nomeado, concorrente/flutuante etc.)			
Licença do software 2 que integra a solução, com nome completo do produto, devendo ser informados sua versão, <i>release</i> e modalidade de licenciamento (usuário nomeado, concorrente/flutuante etc.)			
Licença do software 3 que integra a solução, com nome completo do produto, devendo ser informados sua versão, <i>release</i> e modalidade de licenciamento (usuário nomeado, concorrente/flutuante etc.)			
(...)			
Licença do software N que integra a solução, com nome completo do produto, devendo ser informados sua versão, <i>release</i> e modalidade de licenciamento (usuário nomeado, concorrente/flutuante etc.)			
Hardware			
Equipamento 1 que integra a solução, devendo ser informados marca e modelo.			
Equipamento 2 que integra a solução, devendo ser informados marca e modelo.			
Equipamento 3 que integra a solução, devendo ser informados marca e modelo.			
(...)			
Equipamento N que integra a solução, devendo ser informados marca e modelo.			
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\$

Foram apresentados pela empresa Novell os seguintes apontamentos:

1 - Solicita esclarecimento do texto constante no Termo de Referência (Anexo I), subitem 1.2.1, inciso LXXXV – “ A solução deve permitir a implementação de restrição nos níveis de menu, submenu, subsubmenu, página, campos de uma página e botões da página”. Entende que apenas as aplicações integradas à solução poderão implementar essas restrições, com base nas informações providas pela solução.

Resposta da SEF: A redação será revista pela SEF, da seguinte maneira: “A solução deverá prover informações que permitam às aplicações a ela integradas a implementação de restrição nos níveis de menu, submenu, subsubmenu, página, campos de uma página e botões da página.”

2 - Solicita esclarecimento do texto constante no Termo de Referência (Anexo I), subitem 1.2.1, inciso VI – “A solução deve ser nativamente integrável, interoperável e compatível com as seguintes tecnologias, em termos de execução e de troca de dados”

Pergunta: Execução ou troca de dados? Ou execução e troca de dados?



Resposta da SEF: A redação vai ser corrigida, conforme abaixo:

- VI. “A solução deve ter seus componentes de gerência de identidades e acessos disponíveis nas plataformas Solaris 10 (ou versão superior), ou Red Hat Enterprise Linux AS 4 (ou versão superior) ou Windows 2003 Server (ou versão superior), sendo essa a ordem de preferência para fornecimento desses componentes, sempre que possível, isto é, primeiro Solaris 10 (ou versão superior), depois Red Hat Enterprise Linux AS 4 (ou versão superior) e por último Windows 2003 Server (ou versão superior), admitindo-se o uso de outros sistemas operacionais embarcados em *appliances* para processamento de funcionalidades acessórias, tais como relatórios e auditoria. No que diz respeito aos ambientes em que são executadas aplicações que serão integradas à solução ou que hospedem repositórios que serão utilizados para esse fim, 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 e versão 2008.
 - a.2) Repositórios LDAP v3.
 - b) sistemas operacionais:
 - b.1) Red Hat Enterprise Linux AS versões 4, 5 e 6.
 - b.2) Microsoft Windows 2003 Server e 2008 Server Standard Edition e Enterprise Edition.
 - b.3) SUN Solaris versões 9 e 10.
 - c) Banco de dados:
 - c.1) SGBD ORACLE, versão 10g e 11g.
 - c.2) MS SQL Server 2005 e 2008.
 - d) Software de correio eletrônico:
 - d.1) Microsoft Exchange Server 2007 e 2010.
 - e) Suporte a SPML (Service Provisioning Markup Language);
 - f) Plataforma Java (Java SE Development Kit (JDK) 5.0 e superior e J2EE SDK 1.4 e superior).”

3 - No mesmo inciso VI – “Nas estações de trabalho clientes, com os sistemas operacionais Microsoft Windows XP, Microsoft Windows Vista e Windows 7”;

Sugerido: A redação não prevê adequação da solução para novas versões do sistema operacional Windows que vierem a ser lançadas.

Definido: A fim de estabelecer essa previsão de forma mais clara, sem inviabilizar a participação de soluções que atendem as necessidades da SEF com a qualidade técnica requerida, caso o processo licitatório ocorra exatamente num momento de lançamento de uma nova versão do sistema operacional em questão, sem que tenha havido tempo hábil para adequar a solução de gerenciamento de identidades a ela, foi modificada a redação do item 1.2.3 I, que passou a ser a seguinte: “O sistema deverá ser licenciado na sua versão comercial mais atual, inclusive no que se refere aos componentes que garantem a compatibilidade, a possibilidade de integração e a interoperabilidade com as tecnologias descritas no subitem 1.2.1 - VI acima, nas versões ali descritas ou em versões mais atualizadas, caso existentes.

4 - No mesmo inciso VI – “Nos servidores, com as seguintes plataformas”:



Sugerido: Definir plataforma e definir padrão de integração.

Definido: A redação será alterada, conforme mencionado no comentário ao apontamento 2 da empresa Novell, acima.

5 - No mesmo inciso VI – **b.2)** Microsoft Windows 2000 Server e Microsoft Windows 2003 Server em todas as suas distribuições.

Sugerido: Exclusão do Microsoft Windows 2000 Server

Definido: A redação será alterada. Vide comentário ao apontamento 2 da empresa Novell, acima.

6 - O objeto da contratação poderia ser dividido em 2 lotes, ou seja, a solução e o hardware?

Resposta da SEF: A alternativa sugerida não atende as necessidades desta Secretaria. A SEF/MG tenciona adquirir o hardware e software que compõem a solução de gerenciamento de identidades do mesmo licitante, a fim de evitar conflitos e dúvidas ao atribuir responsabilidades por eventuais problemas ou falhas. Para garantir condições isonômicas de participação no certame, particularmente para licitantes que irão propor o fornecimento de soluções de gerência de identidade cujos fabricantes não são produtores de hardware, será permitido consórcio.

Definido: A redação do objeto não será alterada.

7 - No item 3 do edital - DAS CONDIÇÕES DE PARTICIPAÇÃO, solicita a vedação expressa de participação de consórcio.

Definido: A vedação de consórcios poderia vir a ser um problema para as empresas que não fabricam equipamentos e que teriam de adquiri-los de terceiros, bem como contratar serviços de instalação desses equipamentos. Os representantes da PRODEMGE sugeriram que fosse aberta a possibilidade de subcontratação como forma de obter resultado similar àquele alcançado pela permissão de consórcios. As empresas Novell, CA e Accenture alegaram, contudo, que isso poderia gerar mais custos, comprometendo sua competitividade no certame, devido à necessidade de acréscimo de *markup* sobre os preços de aquisição, inclusive para fazer frente à necessidade de pagamento de tributos, particularmente aqueles que incidem sobre o faturamento, como contribuições sociais, que seriam pagos tanto pelo fabricante do equipamento quanto pela empresa participante do certame. A SEF dispôs-se a avaliar os aspectos jurídicos e de conveniência quanto à participação de consórcios, uma vez que esse tipo de decisão é discricionária, cabendo à administração pública determinar, de maneira justificada, se aceitará ou não esse tipo de participante. A partir de uma primeira avaliação, realizada após a consulta, a SEF entendeu que é conveniente aceitar a participação de consórcios, a fim de garantir isonomia nas condições de participação dos licitantes, uma vez que algumas empresas que fornecem soluções de gerência de identidades são também fabricantes de equipamentos, o que não ocorre com outras.

Foram apresentados pela Computer Associates as seguintes apontamentos:

1- O item XC – ac afirma, em sua descrição, que “Deverá ser criada uma política que descreva os fluxos da informação, declarando suas origens, caminhos e destinos.” e nos seus mecanismos para implementação, que deve-se “Criar uma política que descreva os fluxos da informação, declarando suas origens, caminhos e destinos.”. O representante da empresa Computer Associates entende que a responsabilidade pela criação de uma política de fluxos da informação é da SEF-MG. Esclarece, também, que a ferramenta de gerência de identidades não é capaz de efetuar Data Loss Prevention, uma vez que isso seria característica de um outro tipo de ferramenta. Sugere que a redação seja modificada.

Definido: A redação será modificada, passando a ser a seguinte:

“XC –ac



Descrição: Deverá ser possível configurar na solução fluxos de informação conforme uma política a ser estabelecida, sem implicar na prevenção do vazamento de informações.

Mecanismo de implementação: Configurar na solução fluxos de informação conforme uma política que descreva esses fluxos, declarando suas origens, caminhos e destinos, sem que isso implique na prevenção do vazamento de informações.”

2- O item XC – af afirma, em sua descrição, que “Deverá haver monitoramento e, quando possível, bloqueio de canais dissimulados ou de comunicações ilícitas a partir do sistema e para o sistema” e no respectivo mecanismo de implementação que deverá ser feita “Utilização de solução de firewall e IDS/IPS nas redes onde os sistemas estão instalados. Adicionalmente, utilizar solução de DLP (*Data loss prevention*).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.” Apesar da ressalva feita no texto do mecanismo de implementação, que deixa claro que as ferramentas IDS/IPS e DLP não integram a solução de gestão de identidade a ser fornecida, a empresa Computer Associates sugere a substituição da expressão “utilização” por “integração” no texto do mecanismo de implementação, a fim de evitar mal-entendidos.

Definido: A redação será modificada, passando a ser a seguinte:

“XC – af

Descrição: Deverá ser possível integrar a solução com ferramentas que permitam o monitoramento e, quando possível, bloqueio de canais dissimulados ou de comunicações ilícitas a partir do sistema e para o sistema. Essas ferramentas de monitoramento e bloqueio não fazem parte da solução ofertada.

Mecanismo de implementação: Integração à solução de firewall e IDS/IPS nas redes onde os sistemas estão instalados. Integração à solução de DLP (*Data loss prevention*), caso existente.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.”

3 – O item XXXVIII tem a seguinte redação: “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.” A empresa Computer Associates entende que deve ficar explícita a impossibilidade de troca do identificador único empregado para armazenar todo o histórico de ações de uma identidade, sob pena de perda desse histórico.

Definido: A redação será modificada, passando a ser a seguinte:

“XXXVIII -A solução deve permitir a requisição e a troca do username, login ou nome de usuário de uma identidade, sendo estes distintos do identificador único, sem afetar o registro histórico de ações dessa identidade e sem causar a perda ou alteração de qualquer outro atributo.”

4 - O item LXVIII tem a seguinte redação: “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)”. De acordo com a empresa Computer Associates, essa redação sugere que a solução de gerência de identidades irá utilizar o sistema de segurança em várias plataformas, inclusive mainframe, quando, na verdade, ela tem condições de possuir interoperabilidade com todas essas plataformas, mas não é capaz, necessariamente, de utilizá-las (ou de ser processada/executada nelas).

Definido: A redação será modificada, conforme sugestão apresentada pela PRODEMGE, passando a ser a seguinte:

A solução deve possibilitar a interoperabilidade com sistemas 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).



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

Por fim, os fornecedores foram informados de que os demais questionamentos e sugestões poderiam ser enviados para o e-mail da sgfdcomlicitacao@fazenda.mg.gov.br até dia 31.10.11, para análise e alterações do edital, se fosse o caso. Nada mais havendo a tratar, encerrou-se a sessão.