TRUE ACCESS

SECPL
Fl. 629
Rub.

Brasília/DF, 26 de Março de 2010.

À

CÂMARA DOS DEPUTADOS
COMISSÃO PERMANENTE DE LICITAÇÃO
Brasília - DF

Ref.: EDITAL DO PREGÃO ELETRÔNICO Nº 52/2010

Prezados Senhores,

Inicialmente apresentamos a V.Sas., nossos dados cadastrais para eventuais consultas e/ou endereçamento de alguma correspondência.

Razão Social	True Access Consulting S/A
Endereço	SCN Quadra 05, Bloco "A", Nº 50, Sala 516 - Ed. Brasília Shopping – Torre Sul – Brasília-DF
Inscrição Estadual	07.401.321/001-03
CNPJ	03.369.656/0001-74
CEP Brasília	70.715-900
Endereço Internet	www.trueaccess.com.br
E-mail	rogerio.barbosa@b2br.com.br
Banco	Itaú nº 341
Agência	0522
Conta Corrente	67522-2
Praça	Brasília – DF
Responsável:	Rogério Barbosa dos Santos (Licitação)
Fone/Fax	(61) 3426-3513 e (61) 3426-3303

Estaremos à disposição para quaisquer esclarecimentos que se façam necessários.

Atenciosamente,

ROGÉRIO BARBOSA DOS SANTOS
Procurador
TRUE ACCESS CONSULTING S/A

TRUE ACCESS

SECPL
Fl. 630
Rub.

Em atendimento ao Edital do Pregão à epígrafe, apresentamos a seguinte proposta de preços:

ITEM	DESCRIÇÃO	MARCA (*)	UN.	QUANT.	PREÇO UNITÁRIO R$	PREÇO TOTAL (A) R$	PREÇO MENSAL R$ = (A)/Quant. de meses
Único	**Licenciamento, instalação, configuração, ativação e garantia de funcionamento e atualização de solução de segurança de estações de trabalho (Endpoints) e servidores de rede, incluindo capacitação operacional.**						
1.1	Funcionalidade de antimalware (servidores de rede), firewall e prevenção de intrusão de estação de trabalho (HIPS)	Symantec PROTECTION SUITE ENTERPRISE EDITION 3.0	liç	1800	24,00	43.200,00	--------
1.2	Funcionalidade de controle de acesso à rede local de computadores	Symantec PROTECTION SUITE ENTERPRISE EDITION 3.0	liç	7500	15,00	112.500,00	--------
1.3	Funcionalidade de criptografia de discos rígidos de estações de trabalho	Symantec ENDPOINT ENCRYPTION FULL DISK 7.0	liç	600	25,00	15.000,00	--------
1.4	Funcionalidade de controle de acesso de dispositivos às portas de comunicação de estações e servidores de rede	Symantec PROTECTION SUITE ENTERPRISE EDITION 3.0	liç	7700	22,00	169.400,00	--------
1.5	Funcionalidade de proteção contra códigos maliciosos no Exchange Server 2003	Symantec MAIL SECURITY FOR MS EXCHANGE 6.0	sv Lic	1 6	30,00	180,00	--------
1.6	Instalação e configuração (Subitens 1.1 a 1.5)	---	sv	1	20.461,97	20.461,97	--------
1.7	Capacitação operacional	---	sv	1	12.038,00	12.038,00	--------
1.8	Garantia de funcionamento e de atualização da solução por vinte e quatro meses (Subitens 1.1 a 1.5)	---	sv	1	31.200,00	31.200,00	1.300,00

1.9	Funcionalidade de antimalware (servidores de rede), firewall e prevenção de intrusão de estação de trabalho (HIPS)	Symantec PROTECTION SUITE ENTERPRISE EDITION 3.0	liç	5900	12,00	70.800,00	--------
1.10	Instalação e configuração (Subitem 1.9)	---	sv	1	2.000,00	2.000,00	--------
1.11	Garantia de funcionamento e de atualização da solução por vinte e um meses (Subitem 1.9)	---	sv	1	16.200,03	16.200,03	771,43
					Preço Total do item único R$	**492.980,00**	--------
Preço total do item único por extenso: Quatrocentos e noventa e dois mil e novecentos e oitenta reais							

A comprovação ponto a ponto, bem como os manuais/declaração do fabricante da solução ofertada estão disponíveis no link abaixo:

http://files.grupotba.com.br/licitacoes/CAMARA_ENDPOINT/Comprovacoes_tecnicas.zip

A documentação será também entregue em CD-Rom juntamente com a proposta original a ser enviada para a Câmara dos Deputados.

(**) O subitem 1.5 está sendo ofertado na seguinte opção: 6 (seis) computadores servidores.

PRAZO DE VALIDADE DA PROPOSTA: 60 (sessenta) dias, contados da data de abertura da licitação

PRAZOS DE ENTREGA DOS COMPONENTES E EXECUÇÃO DOS SERVIÇOS, CONFORME CRONOGRAMA DE ENCADEAMENTO DAS FASES DISPOSTO NO ANEXO N. 4 DO EDITAL.

DO CRONOGRAMA DE ENCADEAMENTO DAS FASES

No cronograma apresentado abaixo, os dias úteis definidos destinam-se a ações de responsabilidade exclusiva da contratada e não incluem os dias corridos despendidos pelo órgão fiscalizador nas análises e aferições necessárias à concessão dos aceites provisórios e/ou definitivo das fases descritas.

Fases	Período 1 (Prazo de execução)	Período 2 (Prazo de execução)	Período 3 (Prazo de execução)	Percentual (*)
Fase 1 - Entrega dos Componentes (subitens 1.1 a 1.5 do item único do objeto da licitação contido no Anexo n. 1) e Capacitação Operacional. (Emissão de Aceite Provisório da Fase 1.)	Quinze dias úteis, contados da data de assinatura do contrato	-----	-----	-----
Fase 2 – Instalação, Configuração e ativação da solução (subitens 1.1 a 1.5 do item único do objeto da licitação contido no Anexo n. 1) (Emissão de Aceite Provisório da Fase 2.)	----	Dez dias úteis, contados da data do aceite provisório da Fase 1	-----	**40%**
Fase 3 – Distribuição das funcionalidades configuradas nos equipamentos em rede (subitens 1.1 a 1.5 do item único do objeto da licitação contido no Anexo n. 1). (Emissão do Aceite Provisório da Solução.)	-----	Sessenta e cinco dias úteis, contados da data do aceite provisório da Fase 2	-----	**30%**
Duração (Fases 1 a 3):Noventa dias úteis				
Fase 4 – Licenciamento, Instalação e Distribuição (subitens 1.9 e 1.10 do item único do objeto da licitação contido no Anexo n. 1) (Emissão do Aceite Definitivo da Solução.)	-----	-----	Quinze dias úteis, contados da data do envio da Ordem de Serviço (**A partir de Junho/2010**)	**30%**

PRAZO DE GARANTIA DE FUNCIONAMENTO E ATUALIZAÇÃO REFERENTE AOS SUBITENS 1.1 A 1.5 DO OBJETO DA LICITAÇÃO: 24 (vinte e quatro) meses contados do Recebimento Provisório da Solução

PRAZO DE GARANTIA DE FUNCIONAMENTO E ATUALIZAÇÃO REFERENTE AO SUBITEM 1.9 DO OBJETO DA LICITAÇÃO: 21 (vinte e um) meses contados da data do Recebimento Definitivo da Solução

Declaramos que os subitens constantes dessa planilha correspondem exatamente às especificações descritas no Anexo n. 2 deste Edital, às quais aderimos formalmente.

Declaramos conhecer e aceitar todas as exigências do Edital e dos anexos da presente licitação.

Declaramos que conhecemos a natureza e as condições de execução dos serviços referentes ao objeto desta licitação.

Declaramos que anexamos a esta proposta o detalhamento da forma de licenciamento de cada componente da solução de segurança das estações de trabalho (Endpoints) e servidores de rede.

Comprovação da conformidade técnica

Caso a comprovação da especificação esteja distribuída por vários manuais, listar o nome dos manuais e atribuir um número a cada um. Na coluna "Manual/Página", atribuir um número a cada manual e informar esse e a(s) página(s) correspondente(s).

Relação de Manuais	
Nome do Documento	Número
24967_12836807-3_GA_DS_SEP_10.08.pdf	1
DS_EndEncryp7.0_11.08.pdf	2
SMSMSE_2007.pdf	3
installation_guide.pdf	4
SEE-FD 7.04 Installation Guide.pdf	5
NAC_Administration_Guide.pdf	6
client_guide.pdf	7
Administration_Guide_SEP11.0.5.pdf	8
NAC_solutions_guide.pdf	9
Enforcer_Implementation_Guide.pdf	10
SEE_FD 7.0.4 Client Administrator Guide.pdf	11
sep ru6.docx	12

SECPL
Fl. 634
Rub.

Especificação	Nº Manual/ Pág	Conf
Gerenciamento via console(s) central(is) de um mesmo fabricante.	1, 2 e 3	1)2-3 2)2 3)39
Máximo de três consoles centrais de gerenciamento.	1, 2 e 3	1)2-3 2)2 3)39
Alta disponibilidade por meio de balanceamento de carga em: - Dois ou mais consoles centrais de gerenciamento em execução em máquinas diferentes. - Dois ou mais consoles centrais de gerenciamento funcionando no modo de *cluster* ativo-ativo ou ativo-passivo.	3, 4 e 5	3)39 4)76 5)11
Armazenamento centralizado de registros (*logs*);	6	294
Download automático de atualizações ou por comando dos administradores a partir do site do fabricante da solução.	6	95
Mecanismo para desinstalação de atualizações de forma centralizada.	6	100-101
Distribuição automática de políticas e atualizações via rede ou por comando pelos administradores.	6	105
Aplicação de políticas segundo os critérios de: Todos os agentes; Grupos de agentes ou estações; Agente ou estação específica.	6	331-332
Personalização das notificações aos usuários para português (Brasil).	7	86
Gerência de todas as funcionalidades da solução, incluindo a gerência remota de todas as funcionalidades do(s) agente(s) local(is), por meio de interface gráfica.	1, 2 e 3	1)2,3 2)2 3)39
Interface gráfica para a geração de relatórios sobre o funcionamento da solução e sobre os dados coletados por meio do(s) agente(s).	6	217-218
Definição de grupos de usuários e equipamentos a serem utilizados nas políticas.	6	46, 53-54
Integração com o Microsoft Active Directory 2003 e superior.	8	301-308
Capacidade de importação e sincronização de usuário, grupos de usuários, máquinas e grupos de máquinas presentes no Active Directory.	6	48
Granularidade para atribuir níveis de acesso de leitura ou controle total das funcionalidades da solução de *Endpoint* aos usuários do(s) console(s).	6	72-74
Sistema de auditoria para registrar todas as ações executadas pelos usuários do(s) console(s) de gerenciamento.	8	245-249
Controle dos intervalos de comunicação entre o(s) console(s) de gerenciamento e o(s) agente(s) local(is)	6	348
Gerar alertas e relatórios contendo a lista de máquinas desatualizadas.	6	167
Defini prazo mínimo para que uma máquina seja considerada desatualizada	6	388
Agente(s) local(is):		
Compatibilidade com Microsoft Windows Vista/XP/2000 Professional em português e Microsoft Windows 2000 Server, Windows Server 2003 e superiores em inglês.	4	37
Instalação e desinstalação de forma automática por meio do(s): console(s) de gerenciamento ou *prompt* de comando (*shell*) ou criação de pacote de instalação no formato .msi ou .exe a ser usado por sistema especializado na distribuição de software.	6	87-88
Operação *off-line* quando não for possível entrar em contato com o(s) console(s) de gerenciamento.	8	157-158 97-98
Continua operando com a última política recebida enquanto não for restabelecida a comunicação com o(s) console(s) de gerenciamento.	8	97-98

Especificação	Nº Manual/ Pág	Conf
Permiti o uso de políticas diferentes quando a estação estiver conectada à rede interna (com acesso ao domínio Active Directory) e quanto estiver conectada a outras redes.	8	65-68

Especificação - AntiMalware	Nº Manual/ Pág	Conf
Prove atualizações, no máximo, diárias das definições de *malware* utilizadas. As atualizações deverão ser obtidas pelo(s) console(s) de gerenciamento e distribuídas ao(s) agente(s) local(is) automaticamente.	9	64
Implementa as seguintes formas de varredura contra *malwares* em memória RAM, arquivos, *Registry* e *cookies*:		
Varredura agendada com definição de horários para a verificação das máquinas.	6	376
Habilitação e desabilitação dos agendamentos.	8	430-431
Agendamentos diários, semanais, ao iniciar o sistema operacional e no logon do usuário.	6	364-365, 428
Varredura tempestiva em uma estação ou grupo de estações, com comando por meio do(s) console(s) de gerenciamento.	6	202
Varredura em tempo real (*on-access scanner*).	6	371-372
Varredura heurística para:Detectar arquivos executáveis que tenham código malicioso ou programas potencialmente indesejados; Procurar vírus desconhecidos.	8	491
Configuração de um período de tempo máximo para as varreduras e cancelamento automático em caso de expiração.	12	1
Execução de varreduras por linha de comando ou a partir de arquivos de *batch* ou scripts.	http://www.symantec.com/connect/forums/symantec-endpoint-protection-command-line-scanner	
Opções para quando uma ameaça for encontrada:		
Ação principal: "Limpar automaticamente", "Nega acesso ao arquivo" ou "Exclui automaticamente" ou ações similares.	7	81-83
Ação secundária: "Negar acesso ao arquivo", "Exclui automaticamente", "Move arquivo para área de quarentena" ou "Continua varredura" ou ações similares.	7	84
Formas de classificação e detecção de programas indesejados:		
Vírus, *spyware*, *adware*, *worms*, discadores, capturadores de digitação (*Keyloggers*), ferramentas de administração remota.	7	46-47
Detecção baseada em nomes de arquivos definidos pelo administrador por meio do(s) console(s) de gerenciamento.	6	498
Exclui da varredura arquivos, diretórios, chaves de *Registry* ou *cookies* específicos definidos pelo administrador.	8	430-431
Opções de exame para todos os tipos de varredura:Todos os arquivos; Extensões pré-definidas contidas em lista inicial de extensões perigosas e permiti a inclusão de outras extensões.	7	58, 65
Cadastra extensões que não devem ser verificadas.	7	90
Verifica arquivos compactados nos formatos mais utilizados em nível configurado pelo administrador da solução de Endpoint e codificados MIME.	7	71-73
Configura tempo máximo de varredura para esses arquivos.	12	1
Varredura de arquivos aninhados (*nested files*), ou seja, verifica arquivos compactados que estejam dentro de outros arquivos compactados.	7	71

Especificação - AntiMalware	**Nº Manual/ Pág**	**Conf**
Configuração do nível máximo de aninhamento de compactadores e ação a ser executada.	7	71-73
Verifica arquivos de macro e verificar macros em arquivos de programas de escritório (*Microsoft Office*, *BrOffice* e similares).	6	383
Definição do uso máximo de CPU pelo(s) agente(s) local(is) para cada varredura agendada.	http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008082509323748	
Manutenção de registros (logs) de todas as ações executadas.	6	187-189
Impede a execução de scripts e programas nas pastas de armazenamento temporário (por exemplo, c:\temp, pastas *temp* privativas dos usuários, "Temporary Internet files").	8	515-516
Classificação "*Advanced*" nos testes do AV-comparatives (www.av-comparatives.org) ou ter sido aprovado em um dos dois últimos testes VB100 da Virus Bulletin (www.virusbtn.com).	http://www.virusbtn.com/vb100/archive/results?vendor=VE4	
Em caso de "falsos positivos", última assinatura de malware será reinstalada.	6	494-496

Especificação - Firewall pessoal	**Nº Manual/ Pág**	**Conf.**
Ativação ou desativação do firewall por máquinas ou grupos de máquinas.	6	331
Importar as configurações de firewall de uma estação de trabalho e aplicá-la a outra estação ou a um grupo de estações.	7	122
Criação, alteração e exclusão de lista autorizada (white list) e não autorizada (black list) de execução de programas. As aplicações da lista autorizada sempre terão permissão de execução nas estações. As aplicações da lista não autorizada nunca terão permissão de execução nas estações.	8	515-516 552-553 444 542-543
Criação, alteração e exclusão de listas autorizada (white list) e não autorizada (black list) de endereços IP. Os endereços da lista autorizada sempre terão permissão de acesso via rede às estações. Os endereços da lista não autorizada nunca terão permissão de acesso via rede às estações.	8	444
Criação e aplicação remota de políticas distintas de firewall a grupos diferentes de máquinas.	6	332
Implementa política que permita que apenas uma interface de rede esteja ativa em cada estação.	8	447-448 513-514
Recursos para impedir o desligamento das políticas de firewall por atacantes ou malware.	6	117
Filtragem por tipo de tráfego, aplicação que envia ou recebe dados e assinaturas de ataques conhecidos.	6	438, 436,440
Por meio da interface gráfica do(s) console(s) de gerenciamento, o firewall possui os seguintes itens de configuração:		
Habilita ou desabilita detecção de intrusão;	6	330
Exibi ou não mensagem de notificação de ataque;	6	483
Quando estiver sob ataque:	6	483
Habilita ou não exibição de mensagem;	6	483
Permite envio de email aos administradores.	6	485
Assinaturas de ataque de Port scan (UDP e TCP), Syn flood e PPTP buffer overflow.	6	459
Regras baseadas em tipo de conexão, protocolos IP e não IP, direção do tráfego de rede, aplicação geradora do tráfego, serviço ou porta usada pelo computador, endereço IP usado no pacote.	6	437,438,439

Especificação - Firewall pessoal	**Nº Manual/ Pág**	**Conf.**
Recurso de duplicação de regras existentes.	6	449
Níveis de proteção baixo, alto e personalizado	8	442-443

Especificação - Host-Based Intrusion Prevention System – HIPS	**Nº Manual/ Pág**	**Conf.**
Regras baseadas em: Protocolos IP e não IP; Direção do tráfego (entrada, saída ou ambas);Tipo de conexão (rede ou sem fio); Aplicações que geraram o tráfego; Serviço ou porta usados pelo computador local;Serviço ou porta usados pelo computador remoto; Endereços IP de origem ou destino; Conteúdo dos pacotes.	8	471-473
Modelos de políticas personalizáveis para aplicações e configurações mais usuais.	6	330
Habilita ou desabilita as políticas em estações ou grupos de estações.	6	331
Definição de políticas para permitir ou bloquear a execução de determinadas aplicações.	6	508
Ações de registrar (*log*) ou impedir execução.	6	508
Configuração de notificações de alerta por email.	6	209
Tipos de bloqueio de execução: Execução de aplicação (criação de processo) e Anexação (*hook*) de código a um processo em execução.	6	509-510
Criação de exceções às políticas (classificar aplicações como confiáveis).	6	528
Assinaturas para proteção contra ataques de rede e atualização periódica.	6	456

Especificação - *Network Access Control* – NAC	**Nº Manual/ Pág**	**Conf.**
Compatibilidade com 802.1x (via software ou hardware - appliances) ou Microsoft Network Access Protection (NAP)	7	139
Bloqueia ou coloca sob regime de quarentena os dispositivos que tentarem se conectar à rede da Câmara dos Deputados e não atenderem aos requisitos de segurança, impedindo o acesso à rede local e recursos compartilhados.	7	139
Conformidade do dispositivo tentando conectar à rede da Câmara, tais como: versão da base de dados de malware, firewall configurado conforme as políticas corporativas e ativo, service packs e patches de segurança do sistema operacional atualizados.	7	136
Identifica os sistemas não gerenciados (que não possuem o(s) agente(s) local(is) instalado(s)) e aplicar políticas específicas para esses sistemas.	6 e 10	6)45 10)84
Define tipos ou grupos de sistemas. Deverá permitir a definição de políticas de conformidade específicas para cada grupo ou tipo de sistema.	6	46
Definição de níveis diferentes de acesso à rede, dependendo da violação da política de acesso que foi identificada.	8	565-568
Configurações de máquinas ou grupos de máquinas isentos das políticas de NAC.	10	359
Remediação automaticamente. A remediação inclui todas as ações necessárias para deixar o sistema conforme a política aplicável.	10	367
Funcionalidade de exibição de mensagens de não conformidade aos usuários, listando os problemas encontrados e procedimentos para restaurar o estado de conformidade da estação.	10	105
Definição de quando avaliar a conformidade de sistemas por meio de varreduras:No início do sistema; Quando um sistema é reconectado à rede ou se houver mudança no estado do adaptador de rede; Quando o console do servidor NAC solicitar.	8	565-568
Agendamento de varredura de clientes gerenciados pelo(s) console(s)	8	572

SECPL
Fl. 638
Rub.

Especificação - *Network Access Control* – NAC	Nº Manual/ Pág	Conf.
de gerenciamento. A solução prove mecanismo para habilitar ou desabilitar o agendamento para grupos de máquinas definidas no(s) console(s) de gerenciamento.		
Mínimo, 2 (dois) modos de funcionamento (*enforcement*): Aplicar (*enforce*) a política, restringindo o acesso à rede; Apenas monitorar e registrar os casos de não conformidade.	10	33
Exportação e importação de políticas de conformidade de *Endpoint*.	6	340-341
Relatórios: Via console de gerenciamento, monitoração do acesso à rede (quantidade de máquinas em conformidade (*compliant*) com as políticas e em não conformidade.	6	166-167,169

Especificação - Criptografia de discos rígidos	Nº Manual/ Pág	Conf.
Método que permita ao administrador recuperar acesso a dados criptografados de forma controlada e somente quando for necessário.	11	30
Método de criptografia persistente, independentemente do sistema de arquivo destino (FAT, FAT32, NTFS).	5	13
Suporte à criptografia de todo o disco rígido (ou de partições completas) com autenticação antes ou durante o pré-carregamento do sistema operacional.	5	68
Implementa o algoritmo AES com chaves de 256 bits conforme o padrão FIPS 197.	5	64
Suporta as recomendações do NIST SP800-111 (*Guide to Storage Encryption Technologies for End User Devices*).	Declaração do Fabricante	
Padrão IEEE 1619.	Declaração do Fabricante	
Uso de *tokens* ou *smart cards* com certificados digitais como mecanismo de autenticação.	5	107

Especificação - Controle de dispositivos	Nº Manual/ Pág	Conf.
Controle de interfaces PCMCIA, USB 1.0, 1.1 e 2.0, Firewire, ATAPI, Serial (COM), Paralela, IrDA, SCSI, Bluetooth.	4	19
Controle de *drives* de disco, *pen* drives, dispositivos de imagem, adaptadores de vídeos, teclados, leitores de smart card, drives de CD-ROM/DVD, mouse e outros dispositivos apontadores, controladores de som, vídeo e jogos, drives de disquete, drives de fita e dispositivos de interface humana (HID), dispositivos ACPI específicos, PDAs (Palm, Windows e similares), controladores de cartão de memória.	8	519-520
Modo de aprendizado para dispositivos que são específicos de um fabricante. O aprendizado deverá permitir que a solução passe reconhecer o dispositivo e possa gerenciá-lo.	8	535-536
Granularidade para que alguns dispositivos específicos sejam permitidos, mesmo que a política geral os bloqueie. A solução possibilita aos administradores permitir o uso dos dispositivos com base em número de série, modelo e/ou fabricante.	6	525-526
Aplicação de políticas específicas para grupos de máquinas e usuários definidos no Active Directory.	6	48
Executa atualização de políticas quando usuário efetuar login.	8	95-96
Manutenção das políticas mesmo que esteja desconectada da rede e sem acesso ao(s) console(s) de gerenciamento.	8	95-96
Permissões de acesso: Leitura;Leitura e escrita;Bloqueio.	8	527-528

Especificação - Antimalware para *Exchange Server* 2003 e superior	Nº Manual/ Pág	Conf.

Especificação - Antimalware para *Exchange Server* 2003 e superior	**Nº Manual/ Pág**	**Conf.**
Integra gerenciamento de antimalware ao(s) console(s) de gerenciamento;	3	100-101
Integração com *Active Directory da Microsoft*;	3	138
Compatibilidade com as *APIs* de varredura de código malicioso da Microsoft listadas em http://support.microsoft.com/kb/823166;	3	59
Atualização automática dos arquivos de assinatura de códigos maliciosos;	3	233
Filtragem de mensagens eletrônicas de entrada e saída;	3	152
Identificação de tipo de arquivo e capacidade de filtragem de busca e remoção de anexos e anexos aninhados em arquivos compactados;	3	14, 154
Recurso de gerenciamento de surtos de código malicioso baseado em regras;	3	194, 198
Aplicação políticas de grupo a usuários como exceção à política global;	3	138-140
Alerta de descarte de mensagens infectadas por código malicioso;	3	30,192
Registros (*logs*) consolidados no(s) console(s) de gerenciamento.	3	219, 221

Brasília/DF, 26 de Março de 2010.

Rogério Barbosa dos Santos
Procurador
Carteira de identidade nº: 1.664.471 SSP/DF
CPF n.º 803.010.611-49

EMPRESA: TRUE ACCESS CONSULTING S.A
SEDE: SCN QD. 05, Bloco A, n. 50, Torre Sul, Sala 516, Ed. Brasília Shopping, Torre Sul, Cep 70.715-900 – Brasília - DF
CNPJ: 03.369.656/0001-74