ATA DE REGISTRO DE PREÇOS Nº 134/2014

PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOS IFSC

Pregão Nº 134/2014 – SRP
Processo nº 23292.010897/2014-51

O INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA, CNPJ nº 11.402.887/0001-60, Rua 14 de Julho, 150 – Enseada dos Marinheiros – Coqueiros, Florianópolis/SC – CEP: 88.075-010, doravante denominado apenas CONTRATANTE, neste ato representado pela sua Reitora, Sra MARIA CLARA KASCHNY SCHNEIDER, RG nº 3945665-0 - SSP/SC, CPF 591.649.809-87, realizou no site www.comprasnet.gov.br Pregão Eletrônico para Registro de Preços e, nos termos da Lei nº 10.520/02 e os Decretos nº 5.450/05, 7.892/13, Lei nº 8.666/93 e das demais normas aplicáveis, em razão da classificação das propostas apresentadas no **Pregão Eletrônico de Registro de Preços nº 134/2014**, Ata de Julgamento de Preços, divulgada no Comprasnet e homologada pelo Ordenador de Despesas deste IFSC, RESOLVE registrar os preços para a aquisição dos produtos, objeto do Pregão acima citado, que passa a fazer parte desta, tendo sido os referidos preços oferecidos pelas empresas cujas propostas foram classificadas em primeiro lugar no certame acima enumerado.

CLÁUSULA PRIMEIRA – DO OBJETO

A presente Ata tem por objeto assegurar o compromisso de possível contratação entre o IFSC e as empresas vencedoras do certame licitatório referente ao **Pregão Eletrônico nº 134/2014**, cujo objeto é a aquisição de **LICENÇAS PERPÉTUAS DE ANTIVÍRUS,** para atender as necessidades do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, conforme descrito no Anexo I desta Ata e ratificado por todas as empresas vencedoras através das declarações anexas.

CLÁUSULA SEGUNDA – DA VALIDADE DA ATA

A presente Ata de registro de Preços terá a validade de 12 (doze), compreendendo o período de **04/12/2014 à 03/12/2015.**

Subcláusula Primeira – Durante o prazo de validade desta Ata de Registro de Preço, o IFSC não será obrigado a firmar as contratações que dela poderão advir, facultando-se-lhe a realização de licitação específica para a aquisição pretendida, sendo assegurado ao beneficiário do registro preferência de favorecimento em igualdade de condições.
Subcláusula segunda - Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao órgão gerenciador promover as negociações junto aos fornecedores, observadas as disposições contidas na alínea "d" do inciso II do caput do art. 65 da Lei nº 8.666, de 1993.
Subcláusula terceira - A Ata poderá sofrer alterações de preços de acordo com as condições estabelecidas no arts. 18 e 19 do Decreto nº 7.892, de 23 de janeiro de 2013.

CLÁUSULA TERCEIRA – DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

A presente Ata de Registro de Preços poderá ser usada por todos os órgãos da Administração Pública Federal, desde que autorizados pelo IFSC.
Subcláusula Primeira. O preço ofertado pela(s) empresa(s) signatária(s) a presente Ata de Registro de Preços é especificado conforme o Anexo I.
Subcláusula Segunda. Em cada fornecedor decorrente desta Ata, serão observadas, quanto ao preço, as cláusulas e condições constantes do Edital referente a mesma.
Subcláusula Terceira. Em cada aquisição, o preço unitário a ser pago será o constante da proposta apresentada pela(s) empresa(s) detentora(s) da presente Ata, a(s) qual(is) também a integram.

CLÁUSULA QUARTA – DA CLASSIFICAÇÃO DAS PROPOSTAS

A relação do(s) item(ns) com a(s) respectiva(s) empresa(s) ofertante(s) do menor valor por item, a(s) qual(is) terá(ão) preferência de contratação constitui o Anexo I desta Ata.

CLÁUSULA QUINTA – DO LOCAL E PRAZO DE ENTREGA.

Em cada aquisição, o prazo de entrega do objeto desta licitação será aquele definido no edital do pregão eletrônico que originou esta Ata e os quantitativos serão os informados na Autorização de Fornecimento, conforme Anexo IV do Edital.

CLÁUSULA SEXTA – DO PAGAMENTO

Em todas as aquisições, o pagamento será feito por meio de ordem bancária transmitida ao Banco do Brasil, para crédito em banco, agência e conta-corrente indicados pelo contratado até 15 (quinze) dias do aceite na respectiva Nota Fiscal pelo órgão requisitante.
Subcláusula Primeira. Para os produtos com entregas diárias e semanais, o IFSC estimará o consumo mensal e emitirá uma Autorização de Fornecimento, sendo que o pagamento se dará após as entregas das quantidades previstas na referida autorização.

CLÁUSULA SÉTIMA – DA ENTREGA

A entrega dos produtos só estará caracterizada mediante o recebimento definitivo do mesmo, ou seja, o aceite na respectiva Nota Fiscal correspondente pelo fiscal do contrato.
Subcláusula Primeira. O fornecedor ficará obrigado a atender todos os pedidos efetuados durante a vigência desta Ata, mesmo que a entrega deles decorrente estiver prevista para data posterior à do seu vencimento.
Subcláusula Segunda. Os materiais deverão ser entregues acompanhados da Nota Fiscal ou Nota Fiscal Fatura correspondente.

CLÁUSULA OITAVA – DAS PENALIDADES

A licitante que ensejar o retardamento da execução do certame, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, garantido o direito de ampla defesa, ficará impedida de licitar e contratar com a União, e será descredenciada do SICAF, pelo prazo de até 05 (cinco) anos, enquanto perdurarem os motivos

determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade sem prejuízo das multas previstas em edital e no contrato, e das demais cominações legais.
Subcláusula Única. A contratada ficará sujeita, ainda, as penalidades previstas no edital do Pregão que originou esta Ata.

CLÁUSULA NONA – DO REAJUSTE DE PREÇOS

Considerando o prazo de validade estabelecido na Cláusula Segunda da presente Ata, e em atendimento ao §1º, art.28, da Lei Federal 9.069 de 29.6.1995 e demais legislação, é vedado qualquer reajuste de preços.
Subcláusula única. Fica ressalvada a possibilidade de Alteração das condições para a concessão de reajuste em face da superveniência de normas federais aplicáveis à espécie.

CLÁUSULA DÉCIMA – DAS CONDIÇÕES DE RECEBIMENTO

Os materiais objetos desta Ata de Registro de preços serão recebidos pelo requisitante consoante o disposto no art. 73 da Lei 8.666/93 e demais normas pertinentes.

CLÁUSULA DÉCIMA-PRIMEIRA – DO CANCELAMENTO DA ATA DE REGISTRO DE PREÇOS

Esta Ata de Registro de Preços poderá ser cancelada, de pleno direito:

I – Pela Administração, quando:

a- a detentora não cumprir as obrigações constantes desta Ata de Registro de Preços;
b- a detentora não assinar a Ata no prazo estabelecido e a Administração não aceitar a sua justificativa;
c- a detentora der causa a rescisão administrativa de contrato decorrente de registro de preços;
d- em qualquer das hipóteses de inexecução total ou parcial de contrato decorrente de registro de preços;
e- os preços registrados se apresentarem superiores aos praticados no mercado;
f- por razões de interesse público devidamente demonstradas e justificadas pela Administração;
g- a comunicação do cancelamento do preço registrado, nos casos previstos neste Edital, será feita pessoalmente ou por correspondência com aviso de recebimento, juntando-se o comprovante aos autos que deram origem ao registro de preços;
h- no caso de ser ignorado, incerto ou inacessível o endereço da detentora, a comunicação será feita por publicação no Diário Oficial da União, considerando-se cancelado o preço registrado após a publicação.

II- Pelas detentoras, quando:

6.1. mediante solicitação por escrito, comprovarem estar impossibilitadas de cumprir as exigências desta Ata de Registro de Preços;
6.2. o fornecedor poderá solicitar o cancelamento do seu registro de preços na ocorrência de fato superveniente que venha compromete a perfeita execução contratual, decorrente de caso fortuito ou de força maior, devidamente comprovados;
6.3. à solicitação das detentoras para cancelamento dos preços registrados deverá ser formulada com a antecedência de 30 (trinta) dias, facultada à Administração a aplicação das penalidades

previstas na Lei, caso não aceitas as razões do pedido.

CLÁUSULA DÉCIMA-SEGUNDA – DA AUTORIZAÇÃO PARA AQUISIÇÃO E EMISSÃO DAS AUTORIZAÇÕES DE FORNECIMENTO

As aquisições do objeto da presente Ata de Registro de Preço serão autorizadas, caso a caso, pelo Ordenador de Despesas do IFSC.
Subcláusula Primeira. A emissão das autorizações de fornecimento, sua retificação ou cancelamento, total ou parcial serão igualmente autorizados pelo órgão requisitante.
Subcláusula Segunda. Durante o prazo de validade do Registro de Preços, o IFSC poderá ou não contratar o objeto deste pregão.

CLÁUSULA DÉCIMA-TERCEIRA – DAS DISPOSIÇÕES FINAIS E DO FORO.

Integram esta Ata, o Anexo I (preços registrados) e as declarações de concordância das empresas vencedoras.
Esta Ata está vinculada ao Edital do **Pregão Eletrônico para Registro de Preços nº 134/2014** e às propostas aceitas durante a sessão do referido certame pelas empresas relacionadas no Anexo I desta Ata.
Fica eleito o Foro da Justiça Federal, Seção Judiciária Florianópolis para dirimir quaisquer questões decorrentes da utilização da presente ata.
Os casos omissos serão resolvidos de acordo com a Lei 10.520/2002 e Decreto 5.450/2005, Lei 8.666/93 e demais normas aplicáveis.

Florianópolis, 04 de dezembro de 2014.

MARIA CLARA KASCHNY SCHNEIDER
REITORA DO IFSC

Andrei Zwetsch Cavalheiro
2º Substituto Eventual da Reitora do IF-SC
Port. 972, de 26/07/2012, D.O.U. de 28/09/2012

OBS: A adesão das empresas vencedoras a esta Ata se dá pelas Declarações de Concordância anexas.

ANEXO I - DA ATA DE REGISTRO DE PREÇOS

EMPRESAS E PREÇOS REGISTRADOS

Pregão Nº 134/2014 – SRP
Processo nº 23292.010897/2014-51
Relação de empresas vencedoras, contendo a descrição dos itens e preços negociados na sessão do Pregão.

EMPRESA (1)			GUARDA E PIMENTEL LTDA - ME		
ENDEREÇO			AV. TUPI, 2221, SALA 1002 – ED. GOLD CENTER – CENTRO – PATO BRANCO – PR		
CNPJ			**08.983.236/0001-05**		
TELEFONE/FAX			(46) 3025 1660 – 3025 2841		
REPRESENTANTE LEGAL			RICARDO LUIZ PIMENTEL		
CPF			025.188.529-13		
Email			fernandoosmarini@infoprotect.com.br		
ITEM	**UNID.**	**QTD.**	**ESPECIFICAÇÃO**	**Preço Unitário**	**Preço Total**
1	licença	6000	Licenças (perpétuas) de solução de segurança coorporativa (Antivírus) para ultrabooks (notebooks), estações de trabalho e servidores do ambiente Microsoft nos Campi e Reitoria do IFSC com validade de licenciamento e atualização pelo período de 36 (trinta e seis) meses, conforme especificação abaixo:1 - Segurança para Servidores de Arquivos 1.1 – Suporte total aos sistemas operacionais baseados na plataforma Windows: Windows Server 2003, Windows Server 2008 e Windows Server 2012 (ou superior) em todas as suas versões. 1.2 – Suporte total as plataformas 32 e 64 bits; 1.3 – Todas as funcionalidades deste item devem ser ativadas por agente único que facilita a instalação, a configuração e o gerenciamento. O agente deverá ser o mesmo agente do software de Antivírus. 1.4 – Possuir a funcionalidade de Push do Agente para a instalação nas estações de trabalho sem a necessidade de softwares de terceiros para as máquinas logadas no Domínio do IFSC; 1.5 – Rastreamento em tempo real, para arquivos durante entrada e saída (gravação e leitura), com as seguintes opções: a. Limpar arquivos automaticamente; b. Excluir arquivos Automaticamente; c. Negar acesso de arquivos suspeitos e colocá-los em quarentena; 1.6 – Rastreamento manual com interface Windows, customizável, com opção de limpeza. 1.7 – Permitir diferentes configurações de varredura em tempo real baseando-se em processos de baixo ou alto risco, tornando assim o desempenho do produto mais estável. 1.8 – Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo. 1.9 – Detecção de programas maliciosos como spyware, programas de propaganda, ferramentas como password crackers entre outras: a. Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site da Internet, com freqüência (no mínimo diária) e horários definidos pelo administrador; b. Permitir atualização incremental da lista de definições de vírus; 1.10 – Salvar automaticamente as listas de definições de vírus em local especificado na rede, após cada atualização bem-sucedida. 1.11 – Programação de rastreamentos automáticos do sistema com as seguintes opções: a. Escopo: Todos os drives locais, drives específicos, ou pastas específicas; b. Ação: Somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança	29,80	178.800,00

			(quarentena); c. Freqüência: Horária, diária, semanal, mensal; d. Exclusões: Pastas ou arquivos que não devem ser rastreados. 1.12 – Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional; 1.13 – Gerar notificações de eventos de vírus através de alerta na rede; 1.14 – Permitir bloqueio de aplicações pelo nome do arquivo; 1.15 – Possibilidade de reparar o registro do sistema após eliminação de epidemia; 1.16 – Permitir bloqueio de portas; 1.17 – Permitir criação de regras baseadas em processos de sistema; 1.18 – Permitir o bloqueio de compartilhamentos da máquina em caso de epidemia; 1.19 – Possuir proteção contra estouro de buffer; 1.20 – Capacidade de retomar atualizações de definições de vírus e de software do ponto onde foram interrompidas em caso de perda de conexão, sem necessidade de reinicio de todo o processo; 1.21 – Detecção de cookies potencialmente indesejáveis no sistema; 1.22 – O sistema de antispyware deve estar totalmente integrado ao software antivírus utilizando a mesma biblioteca de definições de vírus e demais ameaças; 1.23 – O sistema deve estar integrado ao console de gerenciamento de segurança de sistemas, que também gerencia antivírus, antispyware, antispam e controle de acesso à rede possibilitando uma única e simples interface para gerenciar toda uma solução de segurança. Não deve ser instalado nenhum software adicional a console de gerenciamento para permitir o controle integrado. 1.24 – Possuir proteção contra BOTs; 1.25 – Estar de acordo com as regulamentações GLBA, CA Breach Act 1386, Sarbanes-Oxley e HIPAA; 1.26 – Funcionar tanto no ambiente corporativo como em VPN; 1.27 – Possuir instalação "silenciosa" ou background; 1.28 – Possuir gerenciamento centralizado; 1.29 – Possibilitar a integração de políticas definidas pelo administrador com o usuário local; 1.30 – Instalação automática em maquinas novas na rede, via software de gerencia; 1.31 – Possuir tecnologia de detecção em nuvem, baseada em "fingerprint" de arquivos suspeitos; 2 - Solução para estações de Trabalho 32 bits e 64 bits 2.1 – Suporte a Windows XP, Windows Vista, Windows 7 e Windows 8 (ou superior); 2.2 – Suporte total a plataforma 32 e 64 bits; 2.3 – Todas as funcionalidades deste item devem ser ativadas por agente único que facilita a instalação, a configuração e o gerenciamento. O agente deverá ser o mesmo agente do software de Antivírus. 2.4 – Rastreamento em tempo real, para arquivos durante entrada e saída (gravação e leitura), com as seguintes opções: a. Limpar arquivos automaticamente; b. Excluir arquivos Automaticamente; c. Negar acesso de arquivos suspeitos e colocá-los em quarentena; 2.5 – Rastreamento manual com interface Windows, customizável, com opção de limpeza. 2.6 – Permitir diferentes configurações de varredura em tempo real baseando-se em processos de baixo ou alto risco, tornando assim o desempenho do produto mais estável. 2.7 – Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo. 2.8 – Detecção de programas maliciosos como spyware, programas de propaganda, ferramentas como password crackers entre outros; 2.9 – Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site da Internet, com freqüência (no mínimo diária) e horários definidos pelo administrador; 2.10 – Permitir atualização incremental da lista de definições de vírus; 2.11 – Salvar automaticamente as listas de definições de vírus em local especificado na rede, após cada atualização bem-sucedida; 2.12 – Programação de rastreamentos automáticos do sistema com as seguintes opções: a. Escopo: Todos os drives locais, drives específicos, ou pastas específicas; b. Ação: Somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena); c. Freqüência: Horária, diária, semanal, mensal;		

			d. Exclusões: Pastas ou arquivos que não devem ser rastreados; 2.13 – Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional; 2.14 – Gerar notificações de eventos de vírus através de alerta na rede; 2.15 – Permitir bloqueio de aplicações pelo nome do arquivo; 2.16 – Possibilidade de reparar o registro do sistema após eliminação de epidemia; 2.17 – Permitir o bloqueio de compartilhamentos da máquina em caso de epidemia; 2.18 – Possuir proteção contra estouro de buffer; 2.19 – Capacidade de retomar atualizações de definições de vírus e de software do ponto onde foram interrompidas em caso de perda de conexão, sem necessidade de reinicio de todo o processo; 2.20 – Detecção de cookies potencialmente indesejáveis no sistema; 2.21 – O sistema de antispyware deve estar totalmente integrado ao software antivírus utilizando a mesma biblioteca de definições de vírus e demais ameaças; 2.22 – O sistema deve estar integrado ao console de gerenciamento de segurança de sistemas, que também gerencia antivírus antispyware, antispam e controle de acesso à rede, possibilitando uma única interface para gerenciar toda uma solução de segurança. Não deve ser instalado nenhum software adicional a console de gerenciamento para permitir o controle integrado; 2.23 – Possuir proteção contra BOTs; 2.24 – Possuir instalação "silenciosa"ou background; 2.25 – Possuir gerenciamento centralizado; 2.26 – Possuir integração com a mesma ferramenta de gerencia do antivírus; 2.27 – Possibilitar a integração de políticas definidas pelo administrador com o usuário local; 2.29 – Instalação automática em maquinas novas na rede, via software de gerencia. 2.30 – Possuir tecnologia de detecção em nuvem, baseada em "fingerprint" de arquivos suspeitos; 2.30 – Possuir ferramenta para verificação de reputação de websites. 2.31 – Possibilidade de configuração de bloqueio de acesso aos sites maliciosos pela console de gerenciamento; 2.32 – Possibilidade de criar blacklists e whitelists de urls para estações pela console de gerenciamento; 3 - Módulo para Gerenciamento Centralizado para todos os módulos da solução antivírus 3.1 – Suporte a instalação do servidor na plataforma Windows Server 2003, 2008 e 2012 (ou superior); 3.2 – Suporte total as plataformas 32 e 64 bits. 3.3 – Suportar o gerenciamento de até 25.000 máquinas a partir de um único servidor; 3.4 – Permitir o gerenciamento do servidor através do protocolo TCP/IP e HTTP; 3.5 – Permitir a instalação dos Módulos da Solução a partir de um único servidor; 3.6 – Permitir a alteração das configurações Módulos da Solução nos clientes de maneira remota; 3.7 – Possuir agentes capazes de efetuar a comunicação direta com o banco de dados sem a necessidade de conexão com o servidor de gerenciamento; 3.8 – Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local; 3.9 – Visualização das características básicas de hardware das máquinas; 3.10 – Integração e Importação automática da estrutura de domínios do Active Directory ou LDAP já existentes na rede local; 3.11 – Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do Sistema Operacional ou no Logon na rede; 3.12 – Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado; 3.13 – Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede; 3.14 – Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados; 3.15 – Criação de grupos de máquinas baseadas em regras definidas em função do número IP do cliente; 3.16 – Permitir a criação de grupos virtuais através de "TAGs"; 3.17 – Permitir aplicar as "TAGs" nos sistemas por vários critérios incluindo: produtos instalados, versão de sistema operacional, quantidade de memória entre outros; 3.18 – Forçar a configuração determinada no servidor para os clientes; 3.19 – Caso o cliente altere a configuração, a mesma deverá retornar ao padrão		

			estabelecido no servidor, quando a mesma for verificada pelo agente. 3.20 – A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura usando protocolo de autenticação HTTPS 3.21 – Forçar a instalação dos Módulos da Solução nos clientes; 3.22 – Caso o cliente desinstale os Módulos da Solução, os mesmos deverão ser reinstalados, quando o agente verificar o ocorrido; 3.23 – Customização dos relatórios gráficos gerados; 3.24 – Exportação dos relatórios para os seguintes formatos: HTML, CSV, PDF; 3.25 – Geração de relatórios que contenham as seguintes informações: a. Máquinas com a lista de definições de vírus desatualizada; b. Qual a versão do software instalado em cada máquina; c. Os vírus que mais foram detectados; d. As máquinas que mais sofreram infecções em um determinado período de tempo; e. Os usuários que mais sofreram infecções em um determinado período de tempo; f. Gerenciamento de todos os módulos da suíte; 3.26 – Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local e fora da rede local; 3.27 – Suportar o uso de múltiplos repositórios para atualização de produtos e arquivo de vacina com replicação seletiva; 3.28 – Ter a capacidade de gerar registros/logs para auditoria; 3.29 – A solução de gerenciamento deve ter a capacidade de atribuir etiquetas as máquinas, facilitando assim a distribuição automática dentro dos grupos hierárquicos na estrutura de gerenciamento; 3.30 – A solução de gerenciamento deve permitir acesso a sua console via web; 3.31 – Implementação de Dashboard com medição do nível de atualização do ambiente e o nível de cumprimento de política de segurança previamente definida. 4 . Garantia, Atualização e Serviços 4.1 – O prazo de garantia de atualização do software e suporte técnico da solução deve ser de no mínimo de 36 (trinta e seis) meses, após a entrega. 4.2 – As atualizações de segurança, implantação de hotfix, patches, novos programas (antivírus) e atualizações de versões deverão ser feitas pela EMPRESA VENCEDORA; 4.3 – A EMPRESA VENCEDORA deverá realizar instalação do console de gerenciamento e ministrar treinamento presencial, de no mínimo 2 (duas) horas quando ocorrer a primeira aquisição de licenças pelos câmpus e reitoria do IFSC. A instalação das licenças de segunda aquisição poderá ser feita remotamente; 4.4 – Deverá ser emitido declaração ou certificado com timbre da EMPRESA VENCEDORA com o(s) nome(s) do(s) participante(s) do treinamento. Deve constar data, hora e local, nome do ministrante e objeto do treinamento. 4.5 – Entregar documentação da solução de segurança em mídia digital considerando a instalação (desinstalação) e demais funcionalidades; 4.6 – Para equipamentos que não possuem antivírus, a instalação deverá ser feita pela EMPRESA VENCEDORA. 4.7 - O software de antivírus deverá realizar a desinstalação automática das versões existentes nas máquinas em operação; ou a EMPRESA VENCEDORA deverá realizar a desinstalação e instalação remota ou presencial; 5 - Suporte Técnico 5.1 – Suporte técnico 8x5 (oito horas por dia, cinco dias por semana) na modalidade remoto via telefone, acesso remoto nos servidores e/ou estações de trabalhos, Mensagem Instantânea, Website, e com possibilidade de atendimento on-site nas unidades do IFSC, para casos em que o IFSC julgar necessário, durante o período de validade da atualização, a contar do aceite da licença. 5.2 – A Garantia de tempo de resposta (SLA) será realizada conforme critérios de prioridades abaixo: a. Prioridade A: até 8 horas úteis b. Prioridade B: até 24 horas c. Prioridade C: até 48 horas Serviço NormalFuncionamento ParcialServiço Indisponível CBA 5.3 - O suporte deverá ser prestado pela CONTRATADA ou por empresa especializada e certificada no software proposto indicada pela mesma, por meio de		

			profissional certificado na ferramenta; Condições Gerais - A PROPONENTE deverá apresentar declaração emitida pelo fabricante de que é Revenda Autorizada a comercializar e a prestar suporte técnico à solução ofertada. A declaração deve ser entregue junto com os demais documentos no momento da aceitação da proposta.		
				TOTAL	**178.800,00**

VALOR TOTAL DA ATA	**R$ 178.800,00**