CREDEQ
Centro de Referência e Excelência em Dependência Química
Unidade Aparecida de Goiânia - Prof. Jamil Issy

SUS

SECRETARIA DE ESTADO DA SAÚDE

GOIÁS
ESTADO INOVADOR

EDITAL

Processo de compras Número 031/2017

O CREDEQ – Centro de Referência e Excelência em Dependência Química – Unidade Aparecida de Goiânia – Jamil Issys, - CNPJ: 02.812.043/0012 – 50, torna público que até o dia 13/03/2017 receberá propostas e orçamentos para aquisição dos seguintes serviços ou produtos:

Descrição do objeto (bem ou serviço)	Solução de T.I.
Quantidade:	• Aquisição de Solução de Firewall de Aplicação, compreendendo hardware, software, serviços de instalação e configuração, garantia, suporte técnico e treinamento • Aquisição de solução de Gerenciamento de servidores Windows baseado no Active Directory, compreendendo serviços de consultoria, instalação e configuração, garantia, suporte técnico e treinamento • Aquisição de Solução de backup em nuvem, composta por sistemas destinados a realização do armazenamento e recuperação de dados do sistema de Gestão do CREDEQ-GO, compreendendo implantação, configuração, monitoramento, garantia, suporte técnico e treinamento • Aquisição de Licenças para Antivírus para o parque de tecnologia da informação • Aquisição de serviços de Help Desk, compreendendo serviços de atendimento 1º e 2º nível a usuários finais, remoto e presencial, para suprir as necessidades do órgão, além de prover serviços de suporte técnico as demais soluções, como firewall, Active Directory, Backup em nuvem e atualizações e/ou suporte a solução de antivírus
Especificação dos Serviços	• Conforme Projeto Básico em Anexo
Justificativa: Para segurança da informação, controle de acesso aos computadores e servidores, manutenção preventiva e corretiva nos equipamentos adquiridos.	
Regime de Compras	Eventual

As propostas e orçamentos deverão ser enviadas por e-mail para: COMPRAS@credeq-go.org.br, até o dia 13/03/2017 às 09:00 Horas. As propostas físicas deverão ser entregues no dia 13/03/2017 às 09:00, na sede da unidade conforme endereço constante no site.

Na oportunidade, analisando as propostas, orçamentos e após eventual negociação, será eleita a proposta vencedora.

Os interessados deverão ainda apresentar as seguintes certidões, conforme o art. 14 do regulamento de compras:

Art. 14. No caso de pessoa jurídica, deverão ser apresentados pelo fornecedor documentos que comprovem a constituição da empresa e sua regularidade fiscal, através da apresentação dos seguintes documentos:

1. CNPJ (comprovante de inscrição e situação cadastral);

2. Certidões negativas (INSS, FGTS, FAZENDA PÚBLICA DO ESTADO DE GOÁS, FISCO MUNICIPAL, RECEITA FEDERAL, TRABALHISTA); Parágrafo primeiro: Se necessários à completa avaliação do fornecedor, a critério a Diretoria Geral, outros documentos poderão ser exigidos. Parágrafo segundo: Para auferir os dados referentes à representação da pessoa jurídica, deverá ser apresentado CONTRATO SOCIAL e sua última alteração. *AS CERTIDÕES SOLICITADAS ACIMA SERÃO EXIGIDAS TAMBÉM NO ATO DO PAGAMENTO.

OS FORNECEDORES DEVERÃO CONSULTAR O REGULAMENTO DE COMPRAS.

OS FORNECEDORES DEVERÃO INFORMAR O SEU ENQUADRAMENTO FISCAL PARA FINS DE TRIBUTAÇÃO.

Dúvidas e esclarecimentos:
(62) 99364-7580 – Cleydson (horário comercial)

Goiânia, 06 de março de 2017.

Cleydson Carlos de Lima
Gerente de Compras e Logística

PROJETO BÁSICO

SOLUÇÃO DE TI - CREDEQ

1. DO OBJETO

1.1. Aquisição de Solução de *Firewall* de Aplicação, compreendendo *hardware, software,* serviços de instalação e configuração, garantia, suporte técnico e treinamento, conforme abaixo:

1.2 Aquisição de solução de Gerenciamento de servidores Windows baseado no Active Directory, compreendendo serviços de consultoria, instalação e configuração, garantia, suporte técnico e treinamento, conforme abaixo:

1.3. – Aquisição de Solução de backup em nuvem, composta por sistemas destinados a realização do armazenamento e recuperação de dados do sistema de Gestão do CREDEQ-GO, compreendendo implantação, configuração, monitoramento, garantia, suporte técnico e treinamento, conforme abaixo:

1.4 – Aquisição de Licenças para Antivírus para o parque de tecnologia da informação

1.5 – Aquisição de serviços de Help Desk, compreendendo serviços de atendimento 1º e 2º nível a usuários finais, remoto e presencial, para suprir as necessidades do órgão, além de prover serviços de suporte técnico as demais soluções, como firewall, Active Directory, Backup em nuvem e atualizações e/ou suporte a solução de antivírus

2. Das Quantidades:

Descrição	Unid.	Qtde Meses
Serviços de Planejamento, Instalação e configuração de Solução de *Firewall*	1	1
Serviços de planejamento, instalação e configuração de Sistemas de Gerenciamento de servidores Windows baseado no Active Directory	1	1
Serviços de Planejamento, instalação e configuração e monitoramento de solução de backup em nuvem	1	1

Aquisição de Licenças para Antivírus para o parque de TI	60	18
Suporte mensal - Serviços de Firewall	1	18
Suporte Mensal - Serviços de AD	1	18
Suporte e Monitoramento mensal - Serviços de backup	1	18
Serviços de Help Desk, compreendendo serviços de atendimento 1º e 2º nível a usuários finais, remoto e presencial	60	18

3. DA DESCRIÇÃO DA SOLUÇÃO

3.1. A CONTRATADA deverá fornecer as seguintes soluções:

3.1.1 - Serviços de Planejamento, Instalação e configuração de Solução de *Firewall*

- Monitoração de transações em tempo real, tomando como base políticas de controle implementadas ou detecção de anomalias para identificar atividades suspeitas ou não autorizadas;
- Gerenciamento centralizado das políticas de segurança por meio de console WEB;
- Coleta de informações quanto ao acesso a dados, exceções, violações de política e envio de alertas; Capacidade de throughput mínima de 1Gpbs
- Capacidade de armazenamento de 500 GB

3.1.2 - Solução de Firewall de Aplicação

3.1.1. A solução deverá ser provida com 1 (um) equipamento, com função de *firewall* de aplicação (*WAF – Web Application Firewall*), para serem instalados em rack padrão 19";

3.1.2. Implementar alta disponibilidade com tolerância a falhas, sendo admitidas as configurações ativo-ativo ou ativo-passivo;

3.1.3. Proteger 2 (dois) segmentos de rede físicos utilizando duas portas de comunicação para cada um dos segmentos

3.1.4. Inspecionar 1 (um) *Gbps* de tráfego de *application firewall*;

3.1.5. Processar 800 (oitocentos) *Kpps* (milhares de pacotes por segundo);

3.1.6. Analisar tráfego *HTTP*/0.9, *HTTP*/1.0 e *HTTP*/1.1;

3.1.7. Restringir métodos *HTTP/HTTPS* permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de *cookies*;

3.1.8. Permitir as seguintes opções de implementação:

3.1.9. Monitoramento (*sniffing*);

3.1.10. *Proxy* (reverso);

3.1.11. Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento;

3.1.12. Quando em modo "monitoramento" (*sniffing*), realizar análise e avaliação do tráfego, gerar relatórios com os dados analisados e simular bloqueios para efeitos de avaliação;

3.1.13. Proteger contra ataques automatizados, incluindo *bots* e *web scraping*, identificando comportamento não humano, navegadores operados por *scripts* ou qualquer outra forma que não operados por humanos;

3.1.14. Bloquear ataques aos servidores de aplicação, por meio dos seguintes recursos:

3.1.15. Identificar, isolar e bloquear ataques sofisticados sem impactar nas transações das aplicações;

3.1.16. Identificar, isolar e bloquear ataques sofisticados para os protocolos: *HTTP* e *HTTPS*;

3.1.17. Permitir a utilização de modelo positivo de segurança para proteger contra ataques às aplicações *HTTP* e *HTTPS*, além de proteger contra ataques conhecidos aos protocolos *HTTP* e *HTTPS*;

3.1.18. Bloquear de imediato o tráfego ou a sessão quando detectada uma tentativa de ataque;

3.1.19. Bloquear com intermediação e interrupção da conexão;

3.1.20. Criar políticas automáticas que bloqueiam o endereço *IP* que realizar violações;

3.1.21. Utilizar página *HTML* informativa e personalizável como *HTTP Response* aos bloqueios;

3.1.22. Configurar políticas de bloqueio baseadas em requisição *HTTP*, endereço *IP* e usuário de aplicação.

3.1.23. Apenas transações de aplicações validadas devem ser aceitas, o restante das transações deverá ser bloqueado, utilizando bloqueio por nível de aplicação baseado no contexto da sessão do usuário, com privilégios de autorização diferentes, entradas de usuários e tempo de resposta de aplicação;

3.1.24. Identificar e armazenar o ataque acontecido com detalhes, com as seguintes informações:

3.1.25. Nome do ataque;

3.1.26. Qual campo foi atacado;

3.1.27. Quantas vezes esse ataque foi realizado;

3.1.28. Cópia da tentativa do ataque;

3.1.29. Horário do ataque; e

3.1.30. Endereços *IP* que originaram os ataques.

3.1.31. Armazenar informações de identificação dos usuários autenticados nas aplicações;

3.1.32. Suportar *request compression* e *response compression*;

3.1.33. Assinar *cookies* digitalmente e editar endereços de *URL* ("*URL Rewriting*");

3.1.34. Proteger as aplicações de banco de dados contra ataques conhecidos, monitorar e controlar os acessos e atividades relacionadas às bases de dados;

3.1.35. Suportar aplicações que utilizem autenticação com estes métodos:

3.1.36. Autenticação básica;

3.1.37. *NTLM*; e

3.1.38. Certificados *SSL*.

3.1.39. Para as soluções que utilizam *SSL* para transferência de dados, os certificados e pares de chaves pública/privada devem ser importados (atuar como *man-in-the-middle* para tráfego *SSL*);

3.1.40. Possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações, incluindo *URLs*, parâmetros *URLs*, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres, se é um campo obrigatório e ainda se é somente-leitura), *cookies*, arquivos *XML*, ações *SOAP*, e elementos *XML*;

3.1.41. Identificar e criar perfil de utilização dos aplicativos, inclusive desenvolvidos em *Javascript*, *CGI*, *ASP* e *PHP*;

3.1.42. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;

3.1.43. Correlacionar múltiplos eventos de segurança em conjunto para distinguir de forma precisa o tráfego permitido do tráfego malicioso;

3.1.44. Identificar ataques baseados em:

3.1.45. Assinaturas, com atualização diária da base pelo fabricante;

3.1.46. Regras; e

3.1.47. Perfis de utilização.

3.1.48. Detectar ataques de força bruta por meio dos seguintes métodos:

3.1.49. Aumento do tempo de resposta da aplicação monitorada;

3.1.50. Quantidade de transações por segundo (*TPS*), monitorando a quantidade de transações por segundo por endereço *IP*;

3.1.51. Detectar ataques do tipo força bruta em que:

3.1.52. O atacante solicita repetidamente o mesmo recurso;

3.1.53. O atacante realiza repetidas tentativas não autorizadas de acesso; e

3.1.54. São utilizados ataques automatizados de *login*.

3.1.55. Detectar ataques do tipo força bruta que explorem:

3.1.56. Controles de acesso da aplicação (Erro 401 – *Unauthorized*);

3.1.57. Solicitações repetidas ao mesmo recurso, em qualquer parte/*URL* da aplicação;

3.1.58. Aplicações *WEB* que não retornam o erro 401 por meio da identificação de expressão regular no retorno/página de erro da aplicação);

3.1.59. Gerenciamento de sessão (muitas sessões de um único endereço *IP* ou a um *range* de *IPs*); e

3.1.60. Clientes automatizados (robôs, requisições muito rápidas).

3.1.61. Permitir a criação de políticas diferenciadas por aplicação e por *URL*, onde cada aplicação e *URL* poderão ter políticas totalmente diferentes;

3.1.62. Possuir mecanismo para criação dinâmica de política de segurança, com aprendizado automático de padrão de utilização da aplicação, realizado sobre o fluxo de tráfego bi-direcional atravessando o equipamento;

3.1.63. Filtrar e validar funções *XML* específicas da aplicação;

3.1.64. Possibilitar atualização de novas assinaturas para ataques conhecidos;

3.1.65. Apresentar proteção positiva e segura contra ataques, como:

3.1.66. Permitir configurar granularmente, por aplicação protegida, restrições de métodos *HTTP* permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de *cookies*;

3.1.67. Permitir definir regras de tamanho para *upload* de arquivos pelo método *PUT*, com as seguintes restrições:

3.1.68. Tamanho por arquivo;

3.1.69. Tamanho por conjunto de arquivos;

3.1.70. Quantidade de arquivos.

3.1.71. A criação das políticas deve possuir as formas:

3.1.72. Automático por meio da observação do tráfego para a aplicação;

3.1.73. Automático por meio da observação do tráfego de teste; e

3.1.74. Manual.

3.1.75. Suportar os seguintes critérios de decisão para realizar bloqueio ou gerar alerta, sendo que uma política pode conter um ou mais critérios simultaneamente:

3.1.76. Tempo de resposta de uma página *web*;

3.1.77. Tamanho da resposta de uma página *web*;

3.1.78. *User-agent* (navegador);

3.1.79. Usuário;

3.1.80. Horário;

3.1.81. *IP* de origem;

3.1.82. Assinatura de ataque;

3.1.83. Conteúdo do *payload*;

3.1.84. Conteúdo do cabeçalho;

3.1.85. Conteúdo da *cookie*;

3.1.86. Código de *response*;

3.1.87. *Hostname*;

3.1.88. Tipo de protocolo (*HTTP* ou *HTTPS*);

3.1.89. Parâmetro;

3.1.90. Número de ocorrências em determinado intervalo de tempo;

3.1.91. Método *HTTP*.

3.1.92. Permitir criação de assinaturas de ataques;

3.1.93. Reconhecer assinaturas seletivas, e filtros de ataque que devem proteger contra:

3.1.94. Ataques de negação de serviços automatizados;

3.1.95. *Worms* e vulnerabilidades conhecidas;

3.1.96. *Requests* em objetos restritos.

3.1.97. Prevenir contra vazamentos dos códigos dos servidores;

3.1.98. Proteger contra as 10 maiores vulnerabilidades da lista *OWASP*;

3.1.99. Exportar requisições que contém os ataques, nos formatos *PDF* e *CSV*;

3.1.100. Realizar localização geográfica do *IP*, identificando país de origem da requisição;

3.1.101. Aprender o comportamento da aplicação:

3.1.102. Campos, valores, *cookies* e *URLs*;

3.1.103. Políticas sugeridas somente devem ser aplicadas após um período configurável.

3.1.104. Inspecionar e monitorar até a camada de aplicação, todo o tráfego de dados *HTTP*, incluindo cabeçalhos, campos de formulários e conteúdo, além de inspecionar os *requests* e *responses*;

3.1.105. As checagens devem ser realizadas em todos os tipos de entrada de dados, como *URLs*, formulários, *cookies*, campos ocultos e parâmetros, consultas (*query*), métodos *HTTP*, elementos *XML* e ações *SOAP*;

3.1.106. Proteger contra mensagens *XML* e *SOAP* malformadas;

3.1.107. Utilizar o campo *HTTP X-Forwarded-For* sem modificar seu conteúdo de origem, permitindo a diferenciação em ambientes com *NAT*;

3.1.108. Suportar *SSL offload*;

3.1.109. Remover as mensagens de erro do conteúdo que será enviado aos usuários;

3.1.110. Emitir os seguintes relatórios:

3.1.111. Gráfico indicando tipo de ataque;

3.1.112. Gráfico indicando tipo de violação;

3.1.113. Gráfico indicando quais *URLs* foram atacadas;

3.1.114. Gráfico indicando severidade;

3.1.115. Gráfico indicando os endereços *IPs* de origem; e

3.1.116. Gráfico indicando a localização geográfica dos endereços *IPs* de origem.

3.1.117. Permitir a seleção de período para emissão dos relatórios, sendo que devem estar disponíveis os dados dos últimos 90 (noventa) dias;

3.1.118. É administrado por ferramenta com interface gráfica remota segura, a partir de plataforma *Windows 7* e *Windows XP*, atendendo os seguintes requisitos:

3.1.119. Permitir a definição de diferentes níveis de administração, no mínimo, um nível completo e outro somente de visualização de configurações e *logs*;

3.1.120. Permitir a geração das seguintes informações, por período:

3.1.121. Auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;

3.1.122. Informações estatísticas de quantidade de conexões completadas e bloqueadas;

3.1.123. Informações estatísticas de fluxo de tráfego; e

3.1.124. Informações estatísticas de quantidade de sessões ou conexões.

3.1.125.

3.1.3 - Serviços de planejamento, instalação e configuração de Sistemas de Gerenciamento de servidores Windows baseado no Active Directory

3.1.126.

3.1.127. Estudo, planejamento e criação das políticas de acesso

3.1.128. Criação das identidades de acesso

3.1.129. Criação de estruturas de gerenciamento de dados centralizadas

3.1.130. Estruturação de serviços dos servidores, baseado em escalabilidade de acesso

3.1.131. Estruturação de políticas de segurança de dados

3.1.132. Criações de logons únicos e baseados na hierarquia do CREDEQ

3.1.133. Contas de usuários e máquinas centralizadas; -

3.1.134. Configuração de serviços nos servidores para que autentiquem e validem os serviços das estações de trabalho

3.1.135. Estruturação dos serviços dos servidores para controlar domínio

3.1.136. Configuração e gestão dos recursos da rede

3.1.137. Delegação de tarefas administrativas;

3.1.138. Análise e estudo de casos para melhoria nos processos de replicação

3.1.139. Implementação de políticas de utilização do sistema (Group Policies).

3.1.140.

3.1.4 - Serviços de Planejamento, instalação, configuração e monitoramento de solução de backup em nuvem

3.1.141.

3.1.142. Esta solução visa contratar serviço de backup, com salvaguarda dos dados na nuvem, conforme modelo comercialmente conhecido como cloud computing, apenas para salvaguarda dos arquivos e documentos referentes ao sistema de gestão (ERP) do CREDEQ.

3.1.143. A contratada fica obrigada a fornecer todos os softwares e agentes de backup que compõem a solução devidamente licenciados para o volume mínimo de 5 (cinco) Terabytes de origem de dados, não sendo permitida qualquer limitação do licenciamento vinculada à quantidade de hosts, módulos e agentes.

3.1.144. Implementar gerenciamento centralizado de toda a solução, de forma que a gerência de todos os ativos envolvidos no backup seja feita a partir de um único ponto.

3.1.145. Implementar monitoramento e administração remotos da solução de backup a partir de qualquer servidor ou estação de trabalho Windows.

3.1.146. Implementar capacidade de configuração de notificação e especificação de recipientes.

3.1.147. Implementar o envio automático de alertas sobre falhas de procedimento de backup ou restore de dados por meio de, no mínimo, mensagens de correio eletrônico compatível com o MS Exchange 2007 SP1 e superior, e Microsoft Outlook 2007 e superior.

3.1.148. Permitir a realização de backup e restore de servidores de rede independentemente da localização física dos servidores ou do datacenter

3.1.149. Permitir que backups incrementais ou diferenciais sejam consolidados com a imagem de backup completo anterior, para disco, por meio de políticas pré-definidas e agendadas.

3.1.150. Informar nos logs todas as mídias utilizadas nas rotinas de backup.

3.1.151. Possuir suporte aos protocolos de rede IPv4 para rotinas de backup e restore.

3.1.152. Possuir módulo nativo de Criptografia AES de 128 ou 256-bits.

3.1.153. Possuir funcionalidade para geração de relatórios customizados, utilizando as seguintes categorias: alertas, jobs, mídia, dispositivos e políticas.

3.1.154. Possuir recursos de agendamento de rotinas de backup para datas específicas e recorrentes para dias da semana, dias do mês e intervalo de dias.

3.1.155. Possuir mecanismo que permita a escolha de uma interface de rede secundária para realização do backup.

3.1.156. Permitir a configuração via interface gráfica do software de backup, sem o uso de scripts ou linha de comando para controle do backup.

3.1.157. Permitir a integração com base de dados MS SQL SERVER 2005/2008 e superior permitindo a configuração da política de backup on-line por meio da interface gráfica do software de backup, sem o uso de scripts ou linha de comando para controle do backup.

3.1.158. O software deverá ser ofertado na modalidade de licenciamento perpétuo, ou seja, não poderão ser cobrados quaisquer valores adicionais pelo uso do software durante e após o término do contrato.

3.1.159. A Contratada deverá prover o fornecimento de nuvem com todos os recursos de tecnologia de informação e comunicação necessárias ao backup do sistema de gestão do CREDEQ

3.1.160. Backup em nuvem deverá ser realizado diariamente, em horário a ser definido pela CREDEQ e os dados deverão ser armazenados em local seguro, com disponibilidade de recuperação em até 08 horas.

3.1.161. A disponibilização do link entre a unidade e nuvem será de responsabilidade do CREDEQ. As velocidades dos links dedicados instalados são de exclusiva responsabilidade da contratante

3.1.162.

3.1.5 - Aquisição de Licenças para Antivírus para o parque de TI

3.1.163.

3.1.164. O presente termo de referência descreve a estrutura mínima a ser fornecida para a implantação da solução de antivírus. Caso a CONTRATADA deseje fornecer solução que necessite de hardware adicional (incluindo hardware novo completo, acessórios, periféricos, componentes ou upgrades no hardware existente na CREDEQ), alterações de software (incluindo upgrade de softwares já instalados na CREDEQ ou licenciamento adicional em software existente na CREDEQ) ou configurações (incluindo ajustes em softwares, otimizações, aplicação de correções, alteração de parâmetros ou customizações) adicionais aos descritos nesse termo de referência, deverá assumir os custos com tais itens, sem qualquer ônus para o CREDEQ. Para tais itens adicionais de hardware/software/configurações a EMPRESA CONTRATADA também deverá assumir os custos com serviços, suporte, licenciamento e treinamento, sem ônus para o CREDEQ. A solução de antivírus deverá ser fornecida pronta para a utilização imediata do CREDEQ. Não será permitido qualquer procedimento que configure o desenvolvimento da solução após a contratação. Caso seja identificado tal procedimento, configurando desenvolvimento de solução, a solução não será aceita sendo aplicadas as penalidades cabíveis ao caso.

3.1.165. A solução deverá contemplar ferramentas que façam varreduras periódicas na rede a fim de localizar máquinas que, possivelmente, não estejam com o cliente do antivírus instalado no equipamento. Configurar hora, semana, dia do mês e ainda em horários definidos pelo administrador da rede através de parâmetros de configuração das atualizações automáticas do antivírus.

3.1.166. Deverá permitir a instalação dos softwares sem a necessidade de forçar a reinicialização da máquina.

3.1.167. Deverá possibilitar a atualização do Pacote de Vacinas definidas pelo administrador do sistema de forma automática através de um ou mais sites locais pré-definidos e também pela Internet.

3.1.168. A solução deverá rastrear em tempo real arquivos durante entrada e saída (gravação e leitura) no equipamento. Durante o rastreamento deverá limpar, apagar ou isolar o arquivo infectado conforme a política definida pelo administrador da Solução de Antivírus

3.1.169. A solução deverá rastrear arquivos compactados para, no mínimo, os seguintes formatos: ZIP, ARJ, RAR e Microsoft Compress

3.1.170. Deverá ser possível, a critério do administrador da solução, a seleção de exclusão de pastas e arquivos que não devem ser rastreados.

3.1.171. Deverá permitir ao administrador bloquear os serviços de compartilhamento quando alvo de códigos maliciosos, no momento de uma epidemia, e, após o término desta, restaurar as configurações originais.

3.1.172. Deverá gerar notificações para o administrador de rede quando ocorrer uma epidemia de vírus através de e-mail.

3.1.173. Deverá ser possível a instalação e a desinstalação dos softwares da Solução de Antivírus, de forma automática, remota silenciosa, ou seja, de maneira que o usuário não perceba ou necessite interagir com o

processo de instalação ou desinstalação do produto. Não será considerado como instalação remota acesso a máquina do usuário usando recursos de terceiros como: vnc, remote desktop, etc.

3.1.174. Deverá ser possível instalar, também de forma silenciosa, a Solução de Antivírus nas estações de trabalho através de scripts durante o Login na rede.

3.1.175. Deverá ser possível instalar o agente de forma remota através de credenciais de administrador local ou do domínio.

3.1.176.

3.1.5.1 - PARA O(S) SERVIDOR(ES)

3.1.177.

3.1.178. A Solução de Antivírus deverá prover software capaz de utilizar servidores Microsoft, instalados em plataforma de 32bit e 64bits, como repositório das atualizações do Pacote de Vacinas e como local centralizado de arquivos compartilhados protegidos pela Solução de Antivírus. O sistema servidor deverá estar apto a funcionar, sem nenhuma restrição, com, no mínimo, as seguintes versões Microsoft: Windows Server 2003; Windows Server 2008.

3.1.179. A Solução de Antivírus deverá prover software capaz de utilizar servidores Linux ou Windows, instalados em plataforma de 32bit e 64bits, como repositório das atualizações do Pacote de Vacinas e como local centralizado de arquivos compartilhados protegidos pela Solução de Antivírus. Caso seja Linux, o sistema servidor deverá estar apto a funcionar, sem nenhuma restrição, com, no mínimo, as seguintes versões: Linux Red Hat Enterprise 4.0 ou superior e Suse Linux Enterprise Server 10 ou superior. Caso seja Windows, o sistema servidor deverá estar apto a funcionar, sem nenhuma restrição, com, no mínimo, as seguintes versões: Windows Server 2003 ou superior e/ou Windows 7. Serão instalados até 22 repositórios das atualizações do Pacote de Vacinas.

3.1.180. A Solução de Antivírus deverá gerenciar as estações de trabalho a partir de um ponto único (console central de gerenciamento), com facilidades para instalação, administração, monitoramento, atualização e configuração, seja de um servidor específico ou de um grupo de servidores ou estações de trabalho.

3.1.181. Deverá permitir atualizar o Pacote de Vacinas do servidor central da solução, de forma automática, através da internet, sem que haja intervenção técnica, e, distribuir, também de forma automática, a partir do servidor central, as atualizações para os demais servidores marcados como sendo repositório de assinaturas. Não serão admitidas replicações com base em scripts ou replicações feitas usando artifícios técnicos não homologados e amplamente documentados pelo fabricante da solução através dos manuais técnicos ou ainda usando softwares de terceiros. A replicação deverá estar apta a ocorrer em, no mínimo, 30 servidores remotos.

3.1.182. Deverá permitir a atualização de forma automática através de serviço de Proxy permitindo a configuração de usuário e senha para autenticação no sistema de internet. Deverá ser totalmente compatível com o Proxy "squid" usado na CREDEQ.

3.1.183. Deverá realizar rastreamentos em tempo real, de forma manual e de forma agendada. O agendamento deverá ser feito, de forma centralizada, no servidor Gerente da solução.

3.1.184. Deverá gerar relatório de incidente (logs) centralizado.

3.1.185. Deverá possuir a capacidade de detecção e remoção de vírus de macro em tempo real.

3.1.186. Deverá ser possível definir políticas de bloqueio às funções de configuração do software em servidores remotos

3.1.187.

3.1.5.2 - PARA AS ESTAÇÕES DE TRABALHO

3.1.188.

3.1.189. Deverá permitir instalação e desinstalação da solução de antivírus nativamente e por scripts em plataformas Windows XP Professional e 7 remotamente.

3.1.190. Deverá permitir autodetecção do sistema operacional para instalação da Solução de Antivírus nas estações de trabalho. Não serão admitidas as soluções que necessitem gerar um pacote de instalação específico para cada versão do Windows.

3.1.191. Deverá permitir instalação e atualização automáticas através de login script Internet/Intranet, CD-ROM/DVD, e através de instalação remota de estações com Windows XP Professional e Windows Vista.

3.1.192. A CONTRATADA deverá prever instalação local e presencial em todos os equipamentos da CREDEQ através de técnicos da CONTRATADA devidamente credenciados pelo fabricante do produto ou técnicos do próprio fabricante do produto.

3.1.193. Deverá permitir e estar apto a realizar configuração diferenciada para cada estação de trabalho, grupo de estações, domínio ou grupos de domínios.

3.1.194. Deverá permitir atualização em clientes móveis a partir do site do fabricante do antivírus, ou de outra fonte definida pelo administrador.

3.1.195. Deverá permitir que o rastreamento agendado seja configurado pelo administrador da rede, com frequência diária, em horário definido, para todas as estações, para um grupo ou estações específicas.

3.1.196. A critério do administrador da Solução de Antivírus deverá ser possível o rastreamento manual, solicitado pelo usuário, através de uma interface gráfica.

3.1.197. Deverá permitir detecção heurística, remoção de vírus de macro em arquivos MS-Office em tempo real, sem eliminação do conteúdo dos arquivos.

3.1.198. Deverá permitir gerar notificações customizáveis para o usuário em caso de detecção de vírus.

3.1.199. Deverá permitir que seja configurado bloqueio de acesso às funções de configuração do software nas estações de trabalho.

3.1.200. Deverá permitir exportar o log para o formato Texto e/ou CSV

3.1.201. Deverá permitir atualização e mudanças de configuração em tempo real através do protocolo http ou protocolo próprio que permita a operação.

3.1.202. Deverá possuir ferramenta integrada que permita seu uso de forma automatizada para reparação de danos causados por vírus do tipo "Trojans", sem a necessidade de uma ferramenta externa.

3.1.203. Deverá permitir procurar códigos maliciosos em arquivos potencialmente infectáveis.

3.1.204. Deverá permitir agendar uma verificação na comunicação entre o servidor e as estações.

3.1.205. Deverá permitir proteção e remoção contra spywares em tempo real em plataformas, Windows XP Professional e Windows 7 ou superior

3.1.206. Deverá permitir armazenamento de log de ocorrência de vírus local e no servidor.

3.1.207. Deverá permitir, através do uso de senha e políticas definidas pelo administrador da Solução de Antivírus, impedir a desinstalação não autorizada ou remoção do módulo residente em memória do cliente de antivírus.

3.1.208. Deverá prover proteção à navegação dos usuários bloqueando os sites web de alto risco e suspeitos, e/ou sites que estejam infectados por algum tipo de malware, para estações de trabalho dentro ou fora da rede.

3.1.209. A lista contendo os sites maliciosos deverá ser atualizada diariamente e automaticamente pela EMPRESA CONTRATADA juntamente com o Pacote de Vacinas.

3.1.210.

3.1.5.3 - INSTALAÇÃO E CONFIGURAÇÃO

3.1.211.

3.1.212. A instalação da Solução de Antivírus deverá ser realizada na unidade do CREDEQ.

3.1.213. Os trabalhos deverão ser realizados no período compreendido entre 08 e 17 horas, de segunda a sexta-feira, excluídos os feriados. Caso a EMPRESA CONTRATADA queira realizar atendimentos fora desse horário, deve previamente agendar o horário com o CREDEQ sob pena de não ser atendida. Esse agendamento dependerá da disponibilidade dos técnicos do CREDEQ

3.1.214. A EMPRESA CONTRATADA deverá instalar e configurar a Solução de Antivírus fornecida. Essa instalação e configuração deverão ser realizadas nas dependências do CREDEQ de forma remota ou presencial;

3.1.215. Para os procedimentos de instalação e configuração a EMPRESA CONTRATADA deverá se utilizar de sua própria mão-de-obra e de seus materiais e equipamentos. O CREDEQ somente fará a supervisão dos trabalhos e auxiliará a EMPRESA CONTRATADA no fornecimento de dados essenciais para o cumprimento do objeto;

3.1.216. A EMPRESA CONTRATADA deverá instalar os softwares em todos os equipamentos do CREDEQ, conforme definição e acompanhamento técnico da equipe de TI

3.1.217. É de responsabilidade da EMPRESA CONTRATADA a remoção da solução antiga de antivírus, caso exista nos servidores e estações de trabalho do CREDEQ, de todos os equipamentos localizados na unidade.

3.1.218. Havendo quaisquer impossibilidades técnicas de remover o produto antigo ou instalar produto novo de forma remota ou automatizada caberá à EMPRESA CONTRATADA encaminhar técnicos especializados ao local para proceder a migração.

3.1.219. A EMPRESA CONTRATADA deverá deixar todos os softwares (patches, service packs, etc.) atualizados em todas as máquinas do CREDEQ;

3.1.220. Após a instalação da Solução de Antivírus a EMPRESA CONTRATADA deverá efetuar todos os testes de funcionalidade da solução fornecida incluindo testes de desempenho nos servidores, estações de trabalho e linhas de comunicação;

3.1.221. A instalação física e a integração dos componentes da solução, entre si e com a estrutura de TI do CREDEQ, é responsabilidade da EMPRESA CONTRATADA;

3.1.222. A instalação física e a integração dos componentes da solução com as linhas de comunicação de dados existentes é responsabilidade da EMPRESA CONTRATADA;

3.1.223. Deverão ser configuradas todas as características solicitadas pelo Departamento de TI do CREDEQ, disponíveis na solução fornecida;

3.1.224. A data de início dos serviços será agendada pelo Departamento de TI do CREDEQ após a entrega oficial do produto pela EMPRESA CONTRATADA, sendo comunicada à EMPRESA CONTRATADA através de ordem de serviço;

3.1.225. Os serviços de instalação e configuração deverão ser concluídos pela EMPRESA CONTRATADA dentro do prazo máximo de 60 (sessenta) dias, a contar da data da ordem de serviço. O descumprimento ao prazo citado sujeitará a EMPRESA CONTRATADA a penalidade de multa;

3.1.226.

4. DOS SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO

Os serviços de instalação e configuração da Solução de *Firewall* de Aplicação deverão ser prestados nas dependências do CREDEQ.

O prazo de execução dos serviços de instalação e configuração é de 30 (trinta) dias corridos contados da data da solicitação de início dos serviços.

A CONTRATADA deverá fornecer todos os componentes (cabos, *software, drivers*, etc.) necessários ao perfeito funcionamento das soluções de firewall, antivírus, backup em nuvem e demais serviços demandados.

Deverão ser configuradas todas as características disponíveis nos produtos fornecidos e solicitados pelo CONTRATANTE.

Deverão ser configuradas políticas de segurança para as aplicações a serem definidas pelo CONTRATANTE.

Após todas as instalações e configurações, o CONTRATANTE deverá validar, junto a CONTRATADA, se os serviços foram instalados e configurados de acordo com as necessidades previstas, atestando sua eficiência, sendo gerado este aceite por parte da CONTRATADA e validado pelo administrador do contrato.

5. DOS SERVIÇOS DE HELP DESK (SUPORTE TÉCNICO)

O prazo de prestação do serviço de HELP DESK (SUPORTE TÉCNICO) será de 18 (dezoito) meses

O suporte técnico é todo aquele prestado por telefone, e-mail, Internet ou presencialmente;

A contratada deverá manter central de atendimento para abertura de chamados no horário comercial (das 8 as 18h). A central deverá ser acionada, preferencialmente, por meio do sistema de chamados, através da internet, devendo a empresa disponibilizar abertura de chamados, tanto por sistema de chamados, quanto por e-mail;

O serviço de suporte técnico consiste no atendimento para reparação de falhas e/ou inconsistências detectadas, de forma a garantir o pleno, correto e seguro funcionamento das soluções do CREDEQ (Firewall, backup em nuvem, antivírus e atendimento aos usuários do CREDEQ);

Este serviço deverá ser prestado mediante requisição do CREDEQ, conforme abertura de solicitação no sistema de chamados da CONTRATADA e nas condições e prazos estabelecidos neste Termo de Referência

Todos os prazos para atendimento do suporte técnico começarão a ser contados a partir da abertura do chamado, independentemente da forma de acionamento

O tempo de solução do chamado será suspenso quando houver pendência de responsabilidade do CREDEQ, e será retomado quando a pendência for sanada;

A solução operacional e definitiva do problema técnico deverá ser concluída nos prazos estabelecidos neste Termo de Referência, a serem contabilizados de forma corrida a partir da abertura do chamado, descontando o tempo que ficou sob responsabilidade o CREDEQ;

Entende-se como solução operacional, a disponibilidade do sistema/serviço, ainda que de forma paliativa ou temporária;

Entende-se como solução definitiva, a resolução completa da causa do problema;

A contratada deverá disponibilizar para si e para o CREDEQ permissão de acompanhamento do chamado através de correio eletrônico ou telefone (ligação gratuita), informando o estado do chamado;

Os chamados serão classificados por severidade, de acordo com o impacto no ambiente computacional do CREDEQ.

Os possíveis níveis de severidade são:

- Severidade 1 – Alta – Um sistema crítico, em produção, está parado ou fora de funcionamento, e não há meios de contornar a falha; número significativo de usuários foi afetado ou impacto operacional significativo foi causado;
- Severidade 2 – Média – Um componente da solução está fora de funcionamento. O problema pode ser contornado. Impactos operacionais moderados a pequenos;
- Severidade 3 – Baixa – Dúvidas, problemas na utilização, esclarecimentos da documentação, sugestões, solicitações de desenvolvimento de novas features ou melhorias;

Níveis de serviços são critérios objetivos e mensuráveis estabelecidos com a finalidade de aferir e avaliar fatores como qualidade, desempenho e disponibilidade dos serviços. Para mensurar esses fatores, serão utilizados indicadores relacionados à severidade e ao estado dos chamados, para os quais foram estabelecidas metas quantificáveis a serem cumpridas pelas contratada e pelo contratante, conforme descrito adiante. Uma hora útil é aquela compreendida entre o período de 8h às 18h, de segunda a sexta-feira, excetuando-se feriados nacionais.

- Chamados de severidade 1 serão iniciados em, no máximo, 3 Horas após a sua abertura, e terão seu status atualizado a cada 3 horas;
- Chamados de severidade 2 serão iniciados em, no máximo, 6 horas úteis após a sua abertura, e terão seu status atualizado a cada 8 horas úteis;
- Chamados de severidade 3 serão iniciados em, no máximo, 24 horas úteis após a sua abertura, e terão seu status atualizado a cada 48 horas úteis;
- Todos os chamados, de qualquer severidade, devem ter solução de contorno (solução paliativa) em no máximo 5 (cinco) dias úteis, e solução definitiva em no máximo 10 (dez) dias úteis, excetuando-se os problemas decorrentes de bugs

no código-fonte do sistema, que serão corrigidos nas próximas atualizações da solução;

A contratada não será responsabilizada pelo não atendimento do nível de severidade estabelecido quando o chamado técnico for originado por falha, interrupção ou qualquer outra ocorrência nos serviços prestados pelas concessionárias de serviços de telecomunicações ou energia elétrica, indisponibilidade de dados, inconsistência de dados e informações geradas pelo CREDEQ, infraestrutura e capacidade de ambiente de tecnologia do CREDEQ ou de terceiros, inclusive o tempo necessário à restauração do ambiente após o restabelecimento das condições de operação, não se caracterizando nesses casos a indisponibilidade dos serviços ou inadimplemento da contratada;

Considera-se um problema plenamente solucionado quando os sistemas e serviços forem restabelecidos sem restrições e de forma definitiva, ou seja, quando não se tratar de uma resolução paliativa.

Toda e qualquer intervenção no ambiente produtivo resultante de suporte técnico deve ser executada somente mediante prévia autorização do CREDEQ, a partir de informações claras dos procedimentos que serão adotados/executados pela contratada.

No final do atendimento e resolução da ocorrência, o técnico da contratada realizará, em conjunto com representantes do CREDEQ, testes para verificação dos resultados obtidos, certificando-se do restabelecimento à normalidade e/ou resolução do problema.

Ao término dos testes e do atendimento (fechamento do chamado), a contratada deverá registrar, detalhadamente, por e-mail, as causas do problema e a resolução adotada.

Nos casos em que o atendimento não se mostrar satisfatório, o CREDEQ fará reabertura do chamado, mantendo-se as condições e prazos do primeiro chamado.

A empresa contratada deverá encaminhar ao CREDEQ até o quinto dia útil do mês subsequente ao da prestação dos serviços relatório de fechamento mensal, acompanhado da correspondente nota fiscal/fatura e documentação que comprove a regularidade fiscal da empresa contratada.

O relatório de fechamento mensal deverá conter a relação de chamados abertos pelo CREDEQ até o término do mês anterior e os indicadores de nível de serviço alcançados de cada chamado.

Os serviços de manutenção e assistência técnica deverão ser prestados na modalidade on-site, nas dependências do CREDEQ, em dias úteis, de segunda à sexta-feira, das 8 às 18h, sem prejuízo do telessuporte, e de acordo com a prioridade atribuída pelo CONTRATANTE.

Os serviços de manutenção e assistência técnica serão solicitados mediante a abertura de um chamado efetuado por técnicos da equipe de Tecnologia da Informação do CREDEQ, via Sistema de Chamados do CONTRATANTE, em dia úteis, de segunda à sexta-feira, das 8h às 18h.

Os chamados poderão ser escalados para níveis mais altos ou mais baixos, de acordo com a criticidade do problema. Nesse caso, os prazos de atendimento e de solução do problema serão automaticamente ajustados para o novo nível de prioridade.

Relativamente à manutenção corretiva de hardware:

5.1.1. Os componentes danificados deverão ser substituídos, entregues, instalados e configurados, de modo a deixar o equipamento em perfeitas condições de uso e com todas as funcionalidades operacionais, nas dependências do CREDEQ, nos prazos de solução estabelecidos acima, sem a cobrança de quaisquer custos adicionais (frete, seguro, etc.);

5.1.2. Em caso de impossibilidade do conserto ser realizado nas dependências do CREDEQ, a CONTRATADA deverá providenciar o deslocamento do equipamento, quando necessário, bem como seu retorno ao local de origem, sendo considerado, para todos os efeitos, durante este período, como fiel depositário do mesmo;

5.1.3. Caso o equipamento defeituoso não possa ser consertado em prazo hábil ou apresente problemas de ordem técnica de hardware, o CREDEQ deverá autorizar a CONTRATANTE a retirar o equipamento para encaminhar a uma assistência técnica para avaliação e apresentação de orçamento. Cabe ao CREDEQ a autorização do reparo, baseado em 3 (três) orçamentos. Após a liberação por parte do CREDEQ, fica autorizada a CONTRATANTE a retirar o equipamento das dependências da autorizada e encaminhar para o CREDEQ, realizando as instalações dos softwares necessários para o pleno reestabelecimento das atividades.

A CONTRATADA deve comprovar o vínculo societário ou empregatício do(s) técnico(s) que vier(em) prestar serviços nas dependências do CREDEQ mediante a apresentação:

Os serviços de suporte técnico serão solicitados mediante a abertura de ordens de serviços, observando o seguinte:

5.1.4. As ordens de serviço serão efetuadas por técnicos do departamento de Tecnologia da Informação do CREDEQ, por meio do sistema de chamados da

CONTRATADA ou por meio do sistema disponibilizado pelo CREDEQ, com antecedência de, no mínimo, 1 (um) dia útil;

5.1.5. Constarão das ordens de serviço, entre outros: atividade a ser executada, data e hora para início do atendimento, prazo de entrega e quantidade estimada de horas técnicas que será considerada para fins de pagamento, independentemente do número de profissionais alocados ou do tempo efetivamente gasto;

5.1.6. O prazo de entrega das ordens de serviço poderá ser prorrogado, a critério exclusivo do CREDEQ, caso a CONTRATADA apresente, tempestivamente, razões de justificativa que comprovem a ocorrência de fatos que fogem ao controle da CONTRATADA e impedem sua execução no prazo estabelecido;

5.1.7.

5.1.8.

5.1.9.

6. DAS CONDIÇÕES DE PARTICIPAÇÃO E PONTUAÇÃO

Poderão participar todas as empresas especializadas em serviços profissionais de tecnologia da Informação que possuam conhecimento comprovado em todas as demandas apresentadas no termo de REFERENCIA DO CREDEQ, sendo pontuados os pré-requisitos descritos a seguir:

1. Possuir pelo menos um membro da equipe com certificação Microsoft Windows Server (20 pontos)
2. Possuir um engenheiro de Computação, devidamente capacitado e com sua graduação comprovada (20 pontos)
3. Possuir em seu quadro de colaboradores e/ou sócios, pelo menos um membro com especialização Strictu Sensu (20 pontos)
4. Atestado de capacidade técnica fornecido por pessoa jurídica de direito público ou privado, que comprove experiência profissional mínima de 10 (dez) anos em instalação, migração, gestão e administração em sistemas de proteção (FIREWALL) (20 pontos)
5. Atestado de capacidade técnica fornecido por pessoa jurídica de direito público ou privado, que comprove experiência profissional em administração de redes Windows, bem como suporte e resolução de problemas (10 pontos)
6. Possuir pelo menos dois veículos de propriedade da empresa para fins de atendimento dos chamados (10 pontos)
7. Possuir equipe técnica própria, devidamente qualificada para atendimento via Web, via e-mail, Skype, via fone e onsite, para atendimentos presenciais. (10 pontos)

8. Possuir sistema próprio de chamados (10 pontos)
9. Ter realizado um diagnóstico detalhado do ambiente de Tecnologia do CREDEQ, contendo, neste laudo, as seguintes informações: (10 Pontos)
    - Laudo técnico detalhado das estações de trabalho e todos os sistemas computacionais instalados
    - Laudo técnico detalhado dos servidores
    - Diagnóstico situacional das atuais condições do parque de tecnologia do CREDEQ, bem como uma prévia avaliação das principais demandas e gargalos operacionais.
10. Ter participado e/ou atuado diretamente na reparação e recuperação de desastres de dados, onde a recuperação dos dados tenha sido bem sucedida, devidamente validada e documentada pelos clientes onde ocorreram os desastres em ambientes de backup na NUVEM. (20 pontos)
11. Valor da Proposta de acordo com o ANEXO I – a pontuação sobre os valores das propostas, será calculado da seguinte forma: Menor Valor Apresentado (MVA) dividido pelo valor da proposta em análise (PEA) multiplicado pela pontuação máxima (PM) (50 pontos).

    Exemplo: recebemos 3 propostas com valores globais

    Empresa 1 = R$ 100.000,00

    Empresa 2 = R$ 110.000,00

    Empresa 3 = R$ 150.000,00

    A aplicação da formula:

    Empresa 1 = MVA (100.000,00) / PEA (100.000,00) X PM (50) = 50 pontos

    Empresa 2 = MVA (100.000,00) / PEA (110.000,00) X PM (50) = 45,45 pontos

    Empresa 3 = MVA (100.000,00) / PEA (150.000,00) X PM (50) = 33,33 pontos

7. DA COMUNICAÇÃO ENTRE O CONTRATANTE E A CONTRATADA

As comunicações, solicitações, notificações ou intimações da Administração decorrentes da contratação, serão feitas pelos seguintes meios:

7.1.1. Mensagem por correio eletrônico ("*e-mail*"), para os endereços eletrônicos indicados pelo CONTRATANTE e CONTRATADA, considerando-se recebida, para todos os efeitos legais, quando respondida a mensagem eletrônica ou confirmado o seu recebimento;

7.1.2. Sistema de chamados a ser disponibilizado pela CONTRATADA

7.1.3. Documento entregue pessoalmente, considerando-se recebido, para todos os efeitos legais, na data da ciência aposta no documento;

8. TRANSIÇÃO CONTRATUAL

Todos conhecimentos adquiridos ou desenvolvidos, bem como toda informação produzida e/ou utilizada para a execução do projeto ou serviços contratados, deverão ser transferidos ao CONTRATANTE, ou empresa por ele designada, em até 60 (sessenta) dias após a finalização do Contrato.

O fato de a CONTRATADA ou seus representantes não cooperarem ou reterem qualquer informação ou dado solicitado pelo CONTRATANTE, que venha a prejudicar, de alguma forma, o andamento da transição das tarefas e serviços para um novo prestador, sujeitará a CONTRATADA à responsabilidade em relação a todos os danos causados ao CONTRATANTE por esta falha.

9. DA CONFIDENCIALIDADE

A CONTRATADA deverá manter a mais absoluta confidencialidade sobre materiais, dados e informações disponibilizados ou conhecidos em decorrência da presente contratação, bem como tratá-los como matéria sigilosa;

A CONTRATADA fica terminantemente proibida de fazer uso ou revelação, sob nenhuma justificativa, a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do CONTRATANTE aos quais tiver acesso em decorrência da prestação dos serviços;

A CONTRATADA deverá obedecer às normas sobre confidencialidade e segurança, internas e externas, adotadas

pelo CONTRATANTE, além das cláusulas específicas constantes deste instrumento.

10. DO LOCAL E HORÁRIO DE ENTREGA E PRESTAÇÃO DOS SERVIÇOS:

Os produtos ou serviços deverão ser entregues e prestados nas dependências do CREDEQ, sito Av. Copacabana s/n Setor Expansul, Aparecida de Goiânia – Goiás, Cep: 74.986-260

10.1.1. Os serviços poderão ser prestados de forma remota, a critério do CONTRATANTE.

Preferencialmente, os serviços serão prestados das 08 às 18h.

11. DOS PRAZOS

Os produtos deverão ser entregues no prazo de 45 (quarenta e cinco) dias corridos contados da data de assinatura do contrato.

Os serviços de instalação e configuração deverão ser prestados no prazo de até 60 (sessenta) dias corridos, contados da data de início de execução constante da Ordem de Serviço.

Os serviços de suporte técnico deverão ser prestados pelo período de 18 (dezoito) meses, admitindo-se a sua prorrogação conforme necessidade do CREDEQ e aceite da CONTRATADA.

Os serviços de garantia deverão ser prestados pelo período de 18 (dezoito) meses admitindo-se a sua prorrogação conforme necessidade do CREDEQ e aceite da CONTRATADA.

12. DAS ESCOLHA DA PROPOSTA MAIS VANTAJOSA

Para a escolha da empresa mais vantajosa para atendimento as necessidades do CREDEQ, serão analisados a pontuação do Item 6, que pode chegar ao número máximo de 200 pontos.

Esta análise será feita pela equipe de T.I do CREDEQ juntamente com a Gerencia Administrativa, Gerência de Compras e Assessoria Jurídica, com base no regulamento de compras do CREDEQ que está publicado no site credeq-go.org.br.

ANEXO I

TOMADA DE PREÇOS DETALAHDO

NOME DA EMPRESA:

CNPJ:

PESSOA PARA CONTATO:

TELEFONE PARA CONTATO:

Descrição	Valor Unit.	Unid.	Qtde Meses	Valor Total
• IMPLANTAÇÃO				
Serviços de Planejamento, Instalação e configuração de Solução de *Firewall*		1	1	
Serviços de planejamento, instalação e configuração de Sistemas de Gerenciamento de servidores Windows baseado no Active Directory		1	1	
Serviços de Planejamento, instalação e configuração e monitoramento de solução de backup em nuvem		1	1	
• ANTIVÍRUS				
Aquisição de Licenças para Antivirus para o parque de TI		60	18	
• SERVIÇO MENSAL				
Suporte mensal - Serviços de Firewall		1	18	
Suporte Mensal - Serviços de AD		1	18	

Suporte e Monitoramento mensal - Serviços de backup		1	18	
Serviços de Help Desk, compreendendo serviços de atendimento 1º e 2º nível a usuários finais, remoto e presencial		60	18	
			VALOR GLOBAL	

TOTAL DE IMPLANTAÇÃO:

TOTAL ANTIVIRUS:

TOTAL MENSAL: