

ANEXO I - TERMO DE REFERÊNCIA

1. OBJETO

Aquisição de solução para gestão de vulnerabilidades e auditoria de configuração de ativos de rede, endereços IP, contêineres, ativos em nuvem e aplicações web, assim como serviços de instalação, suporte técnico, atualização e treinamento.

A solução deve permitir descobrir, avaliar, priorizar e corrigir vulnerabilidades/ configurações em toda a infraestrutura de rede, incluindo estações de trabalho, servidores, dispositivos de rede, dispositivos de telecomunicações e dispositivos de segurança, hypervisors, máquinas virtuais, orquestradores de contêineres e nuvens, proporcionando através de única interface para o administrador via um portal web para gerenciamento de todos os ativos, permitindo o gerenciamento centralizado de todos os componentes da solução a partir de um único ponto, sem a necessidade de incorrer em consoles.

A solução deve ser licenciada por Asset (IP e HOST) e deve fornecer recursos de descoberta e inventário ilimitados com acessos ilimitados a agentes, scanners, sensores de contêineres, sensores de descoberta passivos sem licenciamento – custos adicionais.

2. JUSTIFICATIVA

Com a evolução do cibercrime, violação de dados e interrupções de sistemas devido a ataques cibernéticos, a aquisição de solução de gestão de vulnerabilidades, gerenciamento, monitoramento e suporte do ambiente de Segurança da Informação se torna necessária para o Sesc em Minas, visando proporcionar maior segurança no suporte aos projetos da instituição, proteção a nível individual contra ameaças avançadas, maior acompanhamento a necessidades e incidentes de segurança da informação, além de uma gestão do ambiente tecnológico de segurança tecnológica, visando garantir o maior nível possível de segurança aos dados do Sesc em Minas.

3. ESPECIFICAÇÕES DAS AQUISIÇÕES OU SERVIÇOS

3.1. Contratação Global de solução de Segurança em Tecnologia da Informação, compreendendo os itens conforme tabela abaixo:¹

Item	Descrição	UN.	Quantidade
1	Solução de gestão de vulnerabilidades e auditoria de configuração de ativos de rede, estações de trabalho, endereços IP, contêineres, ativos em Nuvem e aplicações. Web (800 licenças de subscrição).	Meses	36

¹ Definimos a contratação Global, haja vista que os itens são correlatos e indissociáveis.

2	Instalação, configuração, testes em produção e ajustes da solução.	Serviço	1
3	Treinamento da Solução de Segurança.	Serviço	1
4	Suporte e gerenciamento da solução por parte da contratada.	Meses	36

3.2. Solução de Gestão de Vulnerabilidade.

3.2.1. O licenciamento da solução de gestão de vulnerabilidades deverá ser realizado para 800 Assets, conforme tabela abaixo.

Item	Quantidade
Ativos de Infra	780
Aplicações Web para o domínio sescmg.com.br	20

3.3. Características Gerais:

3.3.1. A solução deve ser entregue como um serviço Software-as-a-Service (SaaS) e ou híbrido em uma nuvem proprietária do fabricante para todos os seus serviços e aplicativos exigidos neste documento. Serviços fornecidos por nuvens de terceiros não são aceitos e também 100% on-premises.

Todos os serviços da plataforma devem estar disponíveis sob o mesmo padrão de qualidade de serviço 24x7x365 e garantir 99% de disponibilidade.

O ofertante deve oferecer manutenção e atualização constante da plataforma durante todo o período de vigência do contrato de serviço.

As atualizações de serviço devem ser transparentes para o administrador da solução, sem afetar nenhum dos dados armazenados - serviços fornecidos.

Será admitida apenas 1 desconexão por trimestre, por período de tempo não superior a 4 horas do serviço oferecido em janelas de manutenção programada e previamente avisado.

Todas as comunicações entre componentes, transferência de dados e sincronização da solução devem ser criptografadas de ponta a ponta, fazendo uso de no mínimo TLS 1.2, certificados assinados com RSA 2048 bits e algoritmo de assinatura SHA256.

3.3.2. A solução proposta deverá permitir a descoberta e o inventário de todos os ativos conhecidos e desconhecidos que se conectam ao ambiente de TI híbrido (global) da organização, incluindo dispositivos e aplicativos móveis locais, estações de trabalho, servidores, dispositivos de rede / telecomunicações / segurança, nuvens, contêineres, TO e IoT.

3.3.3. Permitir a descoberta de dispositivos, mesmo se o ping - traceroute não for permitido.

3.3.4. Permitir descobrir todos os ativos ligados à rede, mesmo em segmentos com ambientes isolados e em infraestruturas críticas.

3.3.5. Permitir descobrir ativos, oferecendo as seguintes alternativas:

- Varredura de rede não autenticada ativa
- Varredura ativa de rede autenticada
- Agente

3.3.6. A solução deve oferecer inventário de ativos ilimitado para agentes instalados e deve cobrir os seguintes pontos:

- Inventário de ativos de rede local: deve descobrir todos os dispositivos e aplicativos conectados à rede, incluindo servidores, bancos de dados, estações de trabalho, roteadores, dispositivos de segurança e rede, impressoras e dispositivos IoT.
- Inventário de certificados: deve detectar e catalogar todos os certificados digitais TLS / SSL (internos e externos) de qualquer autoridade de certificação.
- Inventário de nuvem: deve permitir o monitoramento de usuários, instâncias, redes, armazenamento, bancos de dados, ACL, ELB e seus relacionamentos para ter um inventário contínuo de recursos e ativos em pelo menos as seguintes plataformas de nuvem pública:
 - Amazon AWS,
 - Google Cloud Platform
 - Microsoft Azure
- Inventário de Container: deve permitir descobrir e ter visibilidade da infraestrutura de containers ativos - inativos, fornecendo informações sobre imagens, registros, containers associados - criados a partir da mesma imagem e hosts / pods e onde estão localizados.
- Inventário de dispositivos móveis: deve permitir a detecção e catalogação de dispositivos móveis, com todos os detalhes de versão do SO (Android, IOS, IpadOS) e hardware do dispositivo, sua configuração e os aplicativos instalados.

3.3.7. A solução deverá possuir capacidade de identificar a instalação de patches e alterações de configuração em registro para comprovar se a vulnerabilidade foi corrigida.

3.3.8. A solução deverá conter nativamente, sem depender de integrações ou softwares terceiros, a funcionalidade de mostrar patches faltantes aos ativos gerenciados.

3.3.9. A solução deverá possuir capacidade de descoberta, identificação e relatórios sobre vulnerabilidades de dispositivo, sistema operacional e software.

3.3.10. A solução deverá ser capaz de realizar priorização por RTI's (indicadores de ameaças, contexto de superfície de ataque).

3.3.11. A solução deverá permitir a geração de relatórios de conformidade baseado nos principais frameworks de mercado (CIS, NIST, entre outros).

3.3.12. A solução deverá oferecer suporte para avaliação de risco e priorização para remediação fornecida pela capacidade de correlacionar a gravidade da vulnerabilidade e o contexto da criticidade dos ativos, usando inteligência em ameaças (Threat Intelligence), técnicas avançadas de análise (analytics). e técnicas avançadas de inteligência e benchmarks.

3.3.13. A solução deverá fornecer suporte às equipes de TI com informações, orientações de priorização e recomendações para correção e configuração de controles de compensação.

3.3.14. A solução deverá ter capacidade de fornecer algum nível ou se conectar a outras ferramentas de gerenciamento de fluxo de trabalho (workflow), como sistemas de bilhetagem, para descobrir, agir e confirmar o tratamento de vulnerabilidades.

3.3.15. A solução deverá possuir a capacidade de avaliar profundamente as portas abertas para identificar os serviços comuns que podem estar em execução em portas não-padrão.

3.3.16. A solução deverá fornecer descoberta de OS (FingerPrint).

3.3.17. A solução deverá suportar a utilização de credenciais e certificados para melhor precisão na descoberta do sistema operacional.

3.3.18. A solução deverá permitir a classificação e priorização de ativos.

3.3.19. A solução deverá permitir a inclusão de ativos em escaneamentos específicos definidos a partir de faixa de IP, endereço CIDR, Hostname, Nome do Grupo de Ativos, Filtro de Criticidade de Ativos, Filtro Geral ou a partir da leitura de arquivo externo.

3.3.20. A solução deverá executar automaticamente verificações de vulnerabilidade relevantes contra os serviços que estão executando em portas não padrão.

3.3.21. A solução deverá permitir a execução automática de varreduras programadas (agendamento de varredura).

3.3.22. A solução deverá possibilitar a criação ou definição de tempo de execução de varredura, garantindo que a varredura não ultrapassará o tempo estabelecido pelo administrador.

3.3.23. A solução deverá permitir que a varredura seja pausada e reiniciada retomando a execução do ponto em que parou.

3.3.24. A solução deverá fornecer capacidade de realizar um escaneamento rápido, permitindo a entrada de um único endereço IP a ser escaneado.

3.3.25. A solução deverá permitir avaliação de ativos não Windows (Unix, Linux, entre outros) a partir do uso de credenciais.

3.3.26. A solução deve permitir detectar hardwares e softwares desatualizados, sem suporte do fabricante - em final de vida útil.

3.3.27. A solução deverá suportar certificação baseada em autenticação quando utilizado SSH.

3.3.28. A solução deverá suportar alternar para credenciais "superusuário", para serem utilizadas quando o acesso privilegiado for necessário.

3.3.29. A solução deverá suportar a integração com cofre de senhas para uso de credenciais dos ativos a serem escaneados.

3.3.30. A solução proposta deve permitir a coleta de informações detalhadas sobre o ativo gerenciado, deve detalhar pelo menos os seguintes dados para cada ativo:

- Serviços em execução
- Software instalado
- Usuários
- Portas abertas
- Nome do host
- FQDN
- IP v4 / v6
- Endereço MAC
- Volumes de disco
- BIOS

3.3.31. A solução deverá ser capaz de analisar vulnerabilidades em servidores e containers na nuvem.

3.3.32. O licenciamento da plataforma deverá ser por ativos: Ativos de rede, Servidores e Estações de trabalho, Servidores em Cloud, Contêineres, Aplicações Web e API, elementos de rede e IOT.

3.3.33. A solução deve permitir a substituição da licença entre ativos da mesma classe, por exemplo, substituir uma aplicação web por outra, ativos de infraestrutura por outros, etc.

3.3.34. A solução deverá possuir no mínimo as seguintes certificações de privacidade e segurança:

- EU-U.S. Privacy Shield
- Framework;
- Swiss-U.S. Privacy
- Shield Framework;
- Cloud Security Alliance
- (CSA) STAR

3.3.35. A solução deverá ser capaz de identificar no mínimo 50.000 CVE'S.

3.3.36. A solução deverá possuir retenção na nuvem de no mínimo 12 meses dos resultados das varreduras realizadas no ambiente.

3.3.37. A solução deverá garantir que os dados de clientes sejam totalmente separados, não possuindo compartilhamento com terceiros.

3.3.38. O fabricante da solução deverá implementar controles de segurança, como Análise de Vulnerabilidade no mínimo semanal, Firewalls, segmentação de rede, e monitoramento de segurança 24/7/365, para garantir a segurança da aplicação.

3.3.39. A solução deve suportar a análise de incidentes e alertas contendo as mínimas características abaixo:

3.3.40. A console de gerenciamento deve ser 100% em nuvem e ou híbrida.

3.3.41. A solução do fabricante deverá permitir o escaneamento a partir de pontos locais na rede da CONTRATANTE (escaneadores locais), assim como em nuvem.

3.3.42. A solução deverá ser licenciada de modo a realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance) e, indicação da relação de uma determinada vulnerabilidade com códigos maliciosos conhecidos (malware).

3.3.43. A solução deverá possuir recurso de varredura ativa, em que o scanner comunica-se com os alvos (ativos) através da rede.

3.3.44. A solução deverá possibilitar, por meio da console, no mínimo 3 (três) métodos de escaneamento:

- Scan ativo;

- Scan com uso de agentes;
- Scanner em nuvem.

3.3.45. A solução deverá garantir que toda vulnerabilidade que possuir CVE associado deve receber uma nota dinâmica da solução de gestão de vulnerabilidades.

3.3.46. A solução deverá possuir uma API abrangente para automação de processos e integração com aplicações terceiras.

3.3.47. A solução deverá ser capaz de fazer a correlação diária de ameaças ativas contra as vulnerabilidades existentes na infraestrutura, incluindo feeds de inteligência de ameaças, tanto de fontes públicas, quanto não gratuitas.

4. A solução deverá permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional.

4.1.1. A solução deverá ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e HTML.

4.1.2. A solução deverá identificar quais portas estão abertas em determinado ativo.

4.1.3. A solução deverá fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento de configurações e vulnerabilidades.

4.1.4. A solução deve incluir a capacidade de programar períodos em que varreduras possam ser executadas em determinados ativos, podendo selecionar no mínimo a frequência da agenda (diário, semanal, entre outras), hora de início e fim da janela, quais ativos serão excluídos.

4.1.5. A solução deverá apresentar o status da vulnerabilidade, demonstrando na interface de gerenciamento se a mesma é nova, persistente, corrigida ou reapareceu no ativo.

4.1.6. A solução deverá possuir obrigatoriamente os perfis administrador e somente leitura;

4.1.7. A solução deverá gerar relatório de vulnerabilidades para Servidores Windows e Unix com path disponível e criticidade alta.

4.1.8. A solução deverá suportar o envio automático de relatórios para destinatários específicos.

4.1.9. A solução deverá permitir definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal e Semanal.

4.1.10. A solução deve ser capaz de unificar em uma mesma visualização informações de vulnerabilidades, inventário de ativos, vulnerabilidades em containers e status de patches de ativos gerenciados.

4.1.11. A solução deverá permitir exportar dados do que está sendo apresentado na tela, no mínimo para:

- Ativos gerenciados pela solução;

- Todas as vulnerabilidades existentes nos ambientes e em quais ativos elas se encontram;
- Vulnerabilidades por ativo gerenciado pela solução;
- Vulnerabilidades de um único ativo;
- Seleção de vulnerabilidade específica e todos os ativos que a possuem;
- Ativos por vulnerabilidade.

4.1.12. A solução deverá identificar e gerar relatório de ativos expostos à determinada vulnerabilidade.

4.1.13. A solução deverá prover relatórios de inteligência de ameaças avançadas mais recentes e indicadores de comprometimento para ajudar o Sesc em Minas a se defender proativamente contra ameaças.

4.1.14. A solução deve apontar a lista com as principais vulnerabilidades com base em riscos selecionados pelo administrador para priorizar a sua correção.

4.1.15. A solução deverá apresentar indicadores específicos referentes à remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo que a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade.

4.1.16. A console de administração deverá possuir controle de acesso no mínimo permitindo usuários com capacidade de somente visualizar as informações.

4.1.17. A solução deverá inventariar o sistema operacional de cada imagem analisada e suas vulnerabilidades encontradas.

4.1.18. A Solução deve possibilitar a análise das aplicações WEB com as seguintes características:

- Habilitar varreduras profundas dinâmicas para descobrir e catalogar todos os aplicativos da web e APIs na rede corporativa externa, redes corporativas internas e instâncias de nuvem.
- Permitir varreduras autenticadas, complexas e progressivas.
- Suportar varreduras programadas de serviços SOAP e REST API.
- Contar com uma API e integração com Jenkins para automação em um ambiente de CI / CD.
- Detectar, identificar, avaliar, rastrear e corrigir os 10 principais riscos OWASP (Top 10), como injeção de SQL, Cross-site script (XSS), XML External Entity (XXE), autenticação interrompida e

configurações incorretas, também ameaças de WASC, vulnerabilidades CWE e CVEs associados em aplicações da web.

- Suportar a capacidade de re-testar uma vulnerabilidade específica que foi detectada anteriormente na aplicação web.
- Gerar tags para facilitar a localização e o uso de ativos de aplicações web encontrados.
- Permitir que se faça a varredura de grandes aplicações da web usando um mecanismo de varredura progressiva, que deve permitir a varredura em estágios incrementais e evitar quaisquer restrições que possam surgir ao tentar fazer a varredura de um aplicativo de uma vez.
- Definir a hora exata de início e duração das verificações.
- Permitir gerenciar várias varreduras de aplicações web, combinando vários scanners para acelerar o processo e obter resultados mais rapidamente.
- Consolidar os dados de varredura automatizada da solução com dados de ferramentas que permitem a avaliação manual de vulnerabilidades por meio do Burp Suite e Bugcrowd, para uma visão unificada de vulnerabilidades de aplicações web detectadas automática e manualmente.

5. Fornecer relatórios resumidos e de varredura do site que podem ser exportados para os formatos HTML e PDF.

- Oferecer suporte à criação de escopos e funções definidos pelo usuário e permitir que as permissões apropriadas sejam atribuídas a cada função.

5.1.1. A solução deverá analisar as camadas (layers) de um container para:

- Identificar containers que tiveram mudanças de arquivos entre a análise e a sua implementação em produção;
- Identificar as devidas tags das imagens avaliadas;
- Informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem;
- Capacidade de testar automaticamente todas as imagens armazenadas, ou previamente testadas, sempre que uma nova vulnerabilidade for publicada e atualizada no banco de dados de vulnerabilidade da solução, sem qualquer tipo de intervenção manual;
- Inventariar os pacotes e bibliotecas e suas respectivas versões e listar as mesmas dentro do relatório de resultados de análise de cada imagem.

5.2. SUPORTE TÉCNICO

5.2.1. Suporte técnico níveis um, dois e três, que contemplam atendimentos básicos, operacionais, avançados e mitigação de problemas, observando a classificação dos problemas reportados, e prazo de conclusão do chamado a contar da abertura do chamado técnico de acordo com o grau de severidade, segundo a classificação abaixo.

- **Severidade 1:** Problemas que tornem a solução inoperante, no prazo de 3 (três) horas; exceto quando houver escalação do chamado junto ao fabricante da Solução. No caso de necessidade de escalação do chamado junto ao fabricante o Sesc em Minas deverá ser notificado imediatamente após a formalização do mesmo e passa a valer então, o tempo de resposta do fabricante, de acordo com as licenças ativas nos equipamentos;
- **Severidade 2:** Problemas ou dúvidas que prejudicam a operação da infraestrutura da solução, mas que não interrompem o acesso aos dados, no prazo de 8 (oito) horas;
- **Severidade 3:** Problemas ou dúvidas que criam algumas restrições à operação da solução, no prazo: 24 (vinte e quatro) horas;
- **Severidade 4:** Problemas ou dúvidas que não afetam a operação da solução, no prazo de 3 (três) dias úteis.

Entende-se por término do atendimento aos chamados de suporte técnico a disponibilidade da solução para uso em perfeitas condições de funcionamento no local onde está instalada.

5.2.2. O suporte técnico deverá ser realizado após solicitação realizada pela equipe do Sesc em Minas através de sistema OnLine para abertura de chamados, onde a CONTRATADA deve prover o acesso irrestrito ao Sesc em Minas;

5.2.3. O Sistema OnLine para abertura de chamados deve informar o número do chamado, histórico do atendimento e tempo de resposta;

5.2.4. O Sistema OnLine deve permitir a abertura de chamados via website e e-mail;

5.2.5. A abertura de chamados e o atendimento à CONTRATADA via Sistema OnLine deverão ser realizados em português.

5.2.6. O regime de atendimento para suporte técnico e monitoramento será de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco dias) no ano.

5.2.7. O Sesc em Minas pode, eventualmente, solicitar atendimento InLoco na sua Sede, localizada na Rua Tupinambás, número 956, Centro – BH/MG, sendo este agendamento acordado entre as partes previamente, não extrapolando a franquia mensal InLoco de 12 (doze) horas;

5.2.8. Os chamados de suporte técnico deverão ser ilimitados;

5.2.9. O Sesc em Minas enviará uma lista de pessoas autorizadas a abrirem chamados de suporte técnico e mantê-la atualizada de acordo com as mudanças no quadro de funcionários;

5.3. TREINAMENTO

5.3.1. A capacitação deverá ser presencial ou na modalidade remoto ao vivo (aula ao vivo e agendada previamente, com participação simultânea do facilitador e alunos), que poderá ser ministrada de forma presencial ou remota no modelo síncrono (ao vivo).

5.3.2. A capacitação deverá ser ministrada em evento único, para no máximo 5 colaboradores do Sesc em Minas.

5.4. GESTÃO DO AMBIENTE DE SEGURANÇA DA INFORMAÇÃO

5.4.1. A CONTRATADA deverá possuir em seu quadro de funcionários ou contrato de trabalho profissionais certificados pelo fabricante da ferramenta de vulnerabilidade e aptos a realizarem as atividades avançadas no gerenciamento dos dispositivos, comprovados por meio de documento idôneo.

5.4.1.1. A cada mês a CONTRATADA deve realizar uma apresentação de riscos do ambiente;

5.4.2. Deve ser de responsabilidade da CONTRATADA analisar as vulnerabilidades no intuito de encontrar riscos para o ambiente e propor melhorias e correções quando estes forem identificados;

5.4.3. A CONTRATADA deve assinar Termo de Confidencialidade e Sigilo, conforme modelo Anexo II deste Termo de Referência, com objetivo de prover a necessária e adequada proteção às informações restritas de propriedade da Contratante reveladas à Contratada em função da prestação dos serviços objeto deste termo, onde a mesma compromete-se a não reproduzir nem dar conhecimento a terceiros das informações restritas reveladas, sem a anuência de forma expressa da Contratante Assinatura do termo de confidencialidade com os funcionários envolvidos da contratada

5.5. LOCAL DA EXECUÇÃO DOS SERVIÇOS

5.5.1. A implantação dos serviços necessários é de total responsabilidade do fornecedor no endereço abaixo:

Local	Endereço	Contato
Sesc Sede	Rua Tupinambás, 956, Centro - Belo Horizonte - MG, 30120-076	Alan da Silva Costa (31) 3270-8162

6. CRONOGRAMA FÍSICO/FINANCEIRO.

6.1. Entregas:

6.1.1. A instalação, configuração, testes em produção e ajustes da solução, referentes ao item 02 deverão ocorrer no prazo de 30 dias úteis após a assinatura do contrato.

6.1.2. As licenças e o suporte, referentes aos itens 01 e 04 deverão estar disponíveis a partir do início da instalação.

6.1.3. O treinamento, referente ao item 03 deverá ser efetuado no prazo de 45 dias úteis após a assinatura do contrato.

6.2. Pagamentos:

Item	Descrição	Pagamento	Quantidade	Pagamento
1	Solução de gestão de vulnerabilidades e auditoria de configuração de ativos de rede, estações de trabalho, endereços IP, contêineres, ativos em Nuvem e aplicações. Web (800 licenças de subscrição).	Parcelas mensais	36	Após a instalação (conforme item 9.1.)
2	Instalação, configuração, testes em produção e ajustes da solução.	Parcela única	1	Após o recebimento (conforme item 9.1.)
3	Treinamento da Solução de Segurança.	Parcela única	1	Após o recebimento (conforme item 9.1.)
4	Suporte e gerenciamento da solução por parte da contratada.	Parcelas mensais	36	Após a instalação (conforme item 9.1.)

7. PRAZO DE VIGÊNCIA

7.1. A vigência do contrato será de 36 (trinta e seis) meses contados da assinatura do contrato, com possibilidade de prorrogação conforme disposto na Resolução do Sesc nº 1.252/12.

8. GESTOR DO CONTRATO

8.1. Coordenador de Tecnologia da Informação

9. CONDIÇÕES GERAIS

SESC – Serviço Social do Comércio | Departamento Regional Minas Gerais | www.sescmg.com.br

Rua Tupinambás, 956 – Centro – Belo Horizonte/MG CEP: 30.120-906 TEL +55 31 3279 1500

9.1. Condições de pagamento

9.1.1. Prazo de pagamento de 30 dias após emissão de Nota Fiscal.

9.1.2. A Nota Fiscal não poderá ser emitida após o dia 20 de cada mês.

9.1.3. Prazo de pagamento: serão realizados nos dias 05,15 e 25 conforme critérios indicados a seguir:

9.1.4. As Notas Fiscais emitidas entre os dias 06 e 15 do mês corrente, serão pagas no dia 05 do mês subsequente;

9.1.5. As Notas Fiscais emitidas entre os dias 16 e 25 do mês corrente, serão pagas no dia 15 do mês subsequente;

9.1.6. Nenhum pagamento será efetuado à Contratada enquanto pendente de liquidação qualquer obrigação contratual, sem que isso gere direito a reajustamento de preços ou correção monetária.

9.2. Subcontratação

9.2.1. É vedado à licitante vencedora ceder, transferir a execução de parte ou de todo o objeto do presente instrumento.

9.3. REAJUSTE

9.3.1. Índice Geral de Preço de Mercado - IGPM.

9.3.1.1. As demais questões acerca de eventual reajuste, estão definidas no Anexo III – Minuta Contratual.

9.3.2. Os reajustes mencionados serão concedidos desde que seja pleiteado formalmente pela Contratada, mediante apresentação de Planilha de Custos e Formação de Preço, e documentação correlata, e será analisado e aprovado pelo Contratante. Esta solicitação deverá ser por escrito e protocolada junto ao Contratante.

9.3.3. Além do previsto nos itens anteriores, os valores poderão ser alterados para restabelecer a relação que as partes pactuaram inicialmente entre os encargos do Contratado e a retribuição para a justa remuneração da obra, serviço ou fornecimento, objetivando a manutenção do equilíbrio econômico-financeiro inicial do contrato, nas hipóteses legais, em que sobrevierem fatos imprevisíveis, ou previsíveis porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, ou, ainda, em caso de força maior, caso fortuito ou fato do príncipe, configurando álea econômica extraordinária e extracontratual.

9.4. PENALIDADES

9.4.1. As condições de aplicação das penalidades serão previstas na minuta contratual.

SESC – Serviço Social do Comércio | Departamento Regional Minas Gerais | www.sescmg.com.br

Rua Tupinambás, 956 – Centro – Belo Horizonte/MG CEP: 30.120-906 TEL +55 31 3279 1500

9.5. RESCISÃO

9.5.1. O Contrato poderá ser rescindido nas hipóteses previstas na minuta contratual.