O LEGISLATIVO

ÓRGÃO OFICIAL DO PODER LEGISLATIVO DE UBERLÂNDIA | MG

ANO XV NO.2191, SEXTA-FEIRA, 18 DE AGOSTO DE 2017 | EDIÇÃO DE HOJE - 05 PÁGINAS

LICITAÇÕES

AVISO DE LICITAÇÃO

A Câmara Municipal de Uberlândia, representada pelo Departamento de Licitações e Compras e seu Pregoeiro, torna público para conhecimento dos interessados, que a empresa Rodoban Segurança e Transporte de valores Ltda apresentou a Interposição de Recurso do Julgamento do Certame Licitatório – Processo Licitatório nº 0012/2017 - Pregão Presencial nº 009/2017. Conforme art. 4º, XVIII, da Lei 10.520/02 fica os demais licitantes intimados para apresentar contrarrazões, em igual número de dias, 3 (três) dias, sendo-lhes assegurada vista imediata dos autos.

Uberlândia, 18 de agosto de 2017.

Andrea Alves
Pregoeira

TERMOS

Termo de Adjudicação e Homologação

O Presidente e o Ordenador de Despesas da Câmara Municipal de Uberlândia, estado de Minas Gerais, no uso de suas atribuições legais, atendendo ao disposto no Art. 4º, inciso XXII da Lei Federal 10520/2002, Art. 7º inciso IV do Decreto Federal 3.555/2000 e Art. 8º Incisos II e III da Portaria 187/2003, no julgamento do Pregão Presencial 017/2017, Processo Licitatório 031/2017, do tipo MENOR GLOBAL, objetivando AQUISIÇÃO DE 250 LICENÇAS ANTIVIRUS COM INSTALAÇÃO E SUPORTE ADICIONAL POR HORA, obedecidas às especificações e características mínimas previstas no Edital correspondente, ADJUDICAM o objeto da licitação à empresa PSYSTEMID Soluções Tecnológicas Ltda., no valor Global de R$ 21.342,50 (Vinte um mil, trezentos e quarenta e dois reais e cinquenta centavos) e HOMOLOGAM o presente processo licitatório para que surta seus efeitos legais.

Resultado da Adjudicação: Item 01: Aquisição de 250 licenças de software antivírus (sendo 240 para estações de trabalho, notebooks, tabletes e 10 para servidores, caso haja essa diferenciação da ferramenta), incluso a instalação e configuração da ferramenta para a Câmara Municipal de Uberlândia, com as seguintes características mínimas: Módulo de proteção anti-malware; Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais: Windows Server 2003 SP2 e posteriores (32/64-bit); Windows XP SP2 / SP3 e posteriores (x86/x64); Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais; Deve ser integrada ao Windows Security Center, quando utilizado plataforma Microsoft; Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, key loggers, programas de propaganda, rootkits, phishing, dentre outros; Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos; Processos em execução em memória principal (RAM); Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell); Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab; Arquivos recebidos por meio de programas de comunicação instantânea (MSN, Skype, Google Talk, dentre outros). Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como Javascript, Vbscript/Activex; Deve possuir detecção heurística de vírus desconhecidos; Deve permitir diferentes configurações de detecção (varredura ou rastreamento): Em tempo real de arquivos acessados pelo usuário; Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo; Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza; Automáticos do sistema com as seguintes opções: Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos; Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena); Frequência: horária, diária, semanal e mensal; Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados; Deve possuir mecanismo de cache de informações dos arquivos já escaneados; Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada; Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus; Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças; Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independente da maneira de como a URL está sendo acessada; Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça; Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante; Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança; Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos; Deve ter possibilidade de análise forense; Deve fazer análise de processos com capacidade para detectar malware por comportamento. Funcionalidade de atualização

Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução; Deve permitir atualização incremental da lista de definições de vírus; Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável; Deve permitir a indicação de agentes para efetuar a função de

replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas; Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento; O servidor da solução de anti-malware, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os agentes replicadores de atualizações e configurações, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização; O agente replicador de atualizações e configurações deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização; Funcionalidade de administração; Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa; Deve possibilitar instalação "silenciosa"; Deve permitir o bloqueio por nome de arquivo; Deve permitir o travamento de pastas e diretórios; Deve permitir o rastreamento e bloqueio de infecções; Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks; Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho; Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente; Deve permitir a desinstalação através da console de gerenciamento da solução; Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada; Deve permitir criação de diversos perfis e usuários para acesso a console de administração; Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante; Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante; Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory ou IP; Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento; Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos, integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante; Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus; Deve prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console de anti-malware não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias; Deve prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web; Deve prover segurança através de SSL para as comunicações entre o servidor e os agentes de proteção; Deve suportar múltiplas florestas e domínios confiáveis do Active Directory; Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio; Deve permitir a criação de usuários locais de administração da console de anti-malware; Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware; Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento; Deve bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador; Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks; Deve permitir a gerência de domínios separados para usuários previamente definidos; Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração; Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto; Funcionalidade de controle de dispositivos. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total; Deve possuir o controle de acesso a drives de mídias de armazenamento como CDROM, DVD, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total; Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão; Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total; Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, CDROM) mesmo com a política de bloqueio total ativa; Módulo de proteção anti-malware para estações Linux Ubuntu. Varredura manual com interface gráfica, personalizável, com opção de limpeza dos malwares encontrados; Varredura manual por linha de comando, parametrizável e com opção de limpeza automática em todos os sistemas operacionais; Capacidade de detecção e remoção de todos os tipos de malware, incluindo spyware, adware, grayware, cavalos de tróia, rootkits, e outros; Detecção e remoção de códigos maliciosos de macro do pacote Microsoft office, em tempo real; O cliente da solução deve armazenar localmente, e enviar para o servidor (para fins de armazenamento) logs de ocorrência de ameaças, contendo no mínimo os seguintes dados: nome da ameaça, caminho do arquivo comprometido (quando disponível), data e hora da detecção, endereço ip do cliente e ação realizada; Geração de cópia de segurança dos arquivos comprometidos antes de realizar o processo de remoção de ameaças. Esta cópia deve ser gravada na máquina local, e o acesso ao arquivo deve ser permitido somente pela solução de segurança ou o administrador; A desinstalação do cliente nas estações de trabalho deverá ser completa, removendo arquivos, entradas de registro e configurações, logs diversos,

serviços do sistema operacional e quaisquer outros mecanismos instalados; Possibilidade de rastrear ameaças em arquivos compactados em, no mínimo, 15 níveis recursivos de compactação; As mensagens exibidas aos usuários devem ser traduzidas para o português do Brasil; Módulo de proteção anti-malware para estações mac-os O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais: Mac os x 10.6.8 (snow leopard) e 10.7 (lion) em processadores 32 e 64 bits; Mac os x Server 10.6.8 e 10.7 em processadores 32 e 64 bits; Mac os x 10.8 (mountain lion) em processadores 64 bits; Suporte ao apple remote desktop para instalação remota da solução; Gerenciamento integrado à console de gerência central da solução; Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos; Permitir a verificação das ameaças da maneira manual e agendada; Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus; Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infecções a arquivos; Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal; Deve possuir no mecanismo de autoproteção as seguintes proteções: Autenticação de comandos ipc; Proteção e verificação dos arquivos de assinatura; Proteção dos processos do agente de segurança; Proteção das chaves de registro do agente de segurança; Proteção do diretório de instalação do agente de segurança. Funcionalidade de HIPS – Host IPS e Host Firewall Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:Windows Server 2003 SP2 e posteriores (32/64-bit); Windows XP SP2 / SP3 e posteriores (x86/x64); Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host ips e host firewall; Todas as regras das funcionalidades de firewall e ips de host devem permitir apenas detecção (log) ou prevenção (bloqueio); Deve permitir ativar e desativar o produto sem a necessidade de remoção; Deve permitir a varredura de portas lógicas do sistema operacional para identificar quais estejam abertas e possibilitando trafego de entrada ou saída; A funcionalidade de host ips deve possuir regras para controle do tráfego de pacotes de determinadas aplicações; Deve prover proteção contra as vulnerabilidades do sistema operacional Windows XP ou posterior, por meio de regras de host ips; Deve efetuar varredura de segurança automática ou sob demanda que aponte vulnerabilidades de sistemas operacionais e aplicações e atribua automaticamente as regras de host ips para proteger a estação de trabalho ou notebook contra a possível exploração da vulnerabilidade; A varredura de segurança deve ser capaz de identificar as regras de host ips que não são mais necessárias e desativá-las automaticamente; Deve prover proteção contra as vulnerabilidades de aplicações terceiras, por meio de regras de host ips, tais como Oracle Java, Abobe PDF Reader, Adobe Flash Player, Realnetworks Real Player, Microsoft Office, Apple Itunes, Apple Quick Time, Apple Safari, Google Chrome, Mozilla Firefox, Opera Browser, MS Internet Explorer, entre outras; Deve permitir a criação de políticas diferenciadas em múltiplas placas de rede no mesmo sistema operacional; Deve permitir a criação de políticas de segurança personalizadas; Deve permitir limitar o número de conexões simultâneas no sistema operacional. Deve permitir a emissão de alertas via smtp e snmp; Deve permitir configuração e manipulação de políticas de firewall através de prioridades; Deve permitir criação de regras de firewall utilizando os seguintes protocolos: Icmp, icmpv6, igmp, ggp, tcp, pup, udp, idp, nd, raw, tcp+udp. Deve permitir criação de regras de firewall por origem de ip ou Mac ou porta e destino de ip ou mac ou porta; Deve permitir a criação de regras de firewall pelos seguintes frame types: lp, ipv4, ipv6, arp, revarp. Deve permitir também escolher outros tipos de frame type de 4 dígitos em hex code; Deve permitir a criação de grupos lógicos através de lista de ip, Mac ou portas; Deve permitir a criação de contextos para a aplicação para criação de regras de firewall; Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar a visualização e gerenciamentos; A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação; Instalação e configuração. A solução deverá ser entregue instalada atualizada e configurada em todos os computadores da Câmara Municipal de Uberlândia. Todas as regras no A.D. deverão ser configuradas pela empresa contratada. Instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado; Atualização automática das vacinas de forma incremental e da versão do software. O horário de atualização deve ser configurável. A atualização deve permitir conexão através de serviço proxy; Desinstalação automática e remota da solução de antivírus proposta e atual na estação, sem requerer outro software ou agente; Possibilitar instalação "silenciosa". Possibilitar instalação sem necessidade de reiniciar a estação de trabalho. Efetuar a instalação automática em máquinas novas na rede via software de gerência. Possibilidade de ativar e desativar o produto sem a necessidade de remoção. Obs.: A instalação e configuração nos servidores de rede deverá ser feita no Departamento de Informática e nos demais equipamentos deverá ser feita pela empresa vencedora de forma remota. Deverá ser disponibilizado arquivo e/ou link de instalação para utilização posterior. Quantidade: 250 Lic. Marca: ESET Endpoint Protection Advanced. Valor Total do item: 19.842,50 (dezenove mil oitocentos e quarenta e dois reais e cinquenta centavos). Item 02 - Suporte adicional por hora (até 10 horas/ano) durante vigência da licença de 12 meses. Quantidade: 10 horas. Valor total: R$1.500,00 (um mil e quinhentos reais). Adjudicado o item acima para a empresa PSYSTEMID Soluções Tecnológicas Ltda., CNPJ: 23.491.765/0001-77.

Uberlândia, 08 de agosto de 2017.

Alexandre Nogueira da Costa
Presidente
Juliano Ribeiro Modesto
1º Secretário / Ordenador de Despesas

PORTARIAS

PORTARIA 416/17
DISPÕE SOBRE A NOMEAÇÃO QUE MENCIONA

O Presidente da Câmara Municipal de Uberlândia, no uso de suas atribuições legais, RESOLVE:

Art. 1º - Fica nomeada a partir de 21 de agosto de 2017, para o cargo de provimento em comissão, a pessoa abaixo relacionada, a ser lotada no gabinete da vereadora Jussara Mendes Lopes Matsuda:

Assessor Parlamentar Cód. ASP – 01
José Gil Dias.

Art. 2º - Esta portaria entra em vigor na data de sua publicação.

Câmara Municipal, 11 de agosto de 2017.

WILSON ARNALDO PINHEIRO
1º Vice-Presidente

ATAS

RESUMO DA ATA DA 4ª REUNIÃO DO 7º PERÍODO DA 1ª SESSÃO ORDINÁRIA, REALIZADA EM QUATRO DE AGOSTO DE 2017 SEXTA-FEIRA. COMPONENTES DA MESA: Presidente – Alexandre Nogueira; 1º Vice-Presidente – Wilson Pinheiro; 2º Vice-Presidente – Ronaldo Alves; 3ª Vice-Presidente – Michele Bretas; 1º Secretário e Ordenador de Despesas – Juliano Modesto; 2ª Secretária – Jussara Matsuda. ABERTURA: Ao quarto dia do mês de agosto de dois mil e dezessete, sexta-feira, o Presidente, Alexandre Nogueira, declarou aberta a presente reunião, fez a leitura bíblica do dia e convidou a todos os presentes para ouvirem o Hino Nacional Brasileiro. APRESENTAÇÃO DE PROJETOS, DEVOLUÇÃO DE PROCESSOS E OUTROS: Foram Considerados Objetos de Deliberação: 01) Projeto de Lei que Institui o Projeto Inscrição Solidária para Corridas, Caminhadas e Ciclismo de Rua de Uberlândia, e dá outras providências, de autoria da Vereadora Michele Bretas; 02) Projeto de Lei que Denomina de Avenida Lucia Aparecida Ferreira do Nascimento o logradouro público que especifica, de autoria do Vereador Doca Mastroiano; 03) Projeto de Lei que Denomina de Rua Isaias Lopes Medeiros o logradouro público que especifica, de autoria do Vereador Doca Mastroiano; 04) Projeto de Lei que Denomina de Rua João Goulart Filho o logradouro público que especifica, de autoria do Vereador Doca Mastroiano; 05) Projeto de Lei que Denomina de Rua Maria de Lourdes dos Anjos o logradouro público que especifica, de autoria do Vereador Doca Mastroiano; 06) Projeto de Lei que Revoga a Lei Municipal n.º 11.919, de 21 de agosto de 2014, que "Desafeta do domínio público e autoriza o município de Uberlândia a alienar por meio de doação o imóvel que menciona, com dispensa de licitação, ao Conselho Regional de Odontologia de Minas Gerais, para o fim que especifica, revoga a Lei nº 11.653, de 20 de dezembro de 2013 e dá outras providências" e sua alteração, de autoria do Prefeito Municipal; 07) Projeto de Lei que Autoriza o município de Uberlândia a efetuar o reparcelamento dos débitos previdenciários relativos a aporte suplementar atuarial determinado pela Lei nº 11.306/2013 com seu Regime Próprio de Previdência Social – RPPS, Instituto de Previdência Municipal de Uberlândia – IPREMU, de autoria do Prefeito Municipal; 08) Projeto de Lei que Altera a Lei nº 10.662, de 13 de dezembro de 2010 e suas alterações, que "Estabelece normas de proteção do patrimônio cultural do município de Uberlândia, revoga as Leis Municipais nºs 9.702, de 20 de dezembro de 2007 e 10.006, de 20 de outubro de 2008, e dá outras providências", de autoria do Prefeito Municipal; 09) Projeto de Lei que Dispõe sobre o incentivo de microcervejarias artesanais e caseiras no município de Uberlândia e dá outras providências, de autoria do Vereador Felipe Felps. Foram encaminhados: PARA COMISSÃO DE LEGISLAÇÃO, JUSTIÇA E REDAÇÃO: 01) Projeto de Lei nº 379/17 que Institui a obrigatoriedade de o Poder Executivo proporcionar tratamento especializado, educação e assistência específicas a todos os autistas, independentemente de idade, no âmbito do município de Uberlândia, de autoria do Vereador Ismar Prado; 02) Projeto de Lei nº 380/17 que Abre crédito suplementar no orçamento da Secretaria Municipal de Desenvolvimento Social, Trabalho e Habitação no valor de R$5.925,00, autoriza a transferência de recursos às entidades que menciona e dá outras providências, de autoria do Prefeito Municipal; 03) Projeto de Lei nº 381/17 que Autoriza a transferência de recursos do orçamento da Secretaria Municipal de Desenvolvimento Social, Trabalho e Habitação à entidade que menciona no valor de R$ 124.000,00, e dá outras providências, de autoria do Prefeito Municipal. ORDEM DO DIA: Foi aprovada a ata da 3ª reunião do 7º período da 1ª sessão ordinária. Foram aprovados os requerimentos, indicações e moções de n°s 8102, 8121, 8178 a 8223, 8225 a 8238, 8240 a 8244, 8246 a 8251, 8254 a 8256, 8258 a 8260/17. PROJETOS EM DISCUSSÃO: Em Discussão Única foram aprovados: 01) Projeto de Lei nº 345/17 que Declara de utilidade pública a entidade de Associação P.A. Dom José Mauro da Fazenda Santa Mônica e Douradinho do município de Uberlândia/MG - ASFMD, de autoria do Vereador Ricardo Santos, aprovado por maioria simples simbólica; 02) Projeto de Decreto Legislativo nº 042/17 que Concede Diploma de Honra ao Mérito à empresa "Sapataria Martoli", de autoria do Vereador Antônio Carrijo, aprovado por maioria simples simbólica. Em 1ª Discussão foi aprovado: Projeto de Lei nº 269/17 que Dispõe sobre o direito ao aleitamento materno nos estabelecimentos de uso coletivo, públicos ou privados, de autoria do Vereador Paulo César, aprovado por maioria simples simbólica. Em 1ª Discussão foi rejeitado: Projeto de Lei nº 303/17 que Altera dispositivo da Lei nº 10.715, de 21 de março de 2011, que Institui o Código Municipal de Saúde, de autoria do Vereador Pastor Átila, rejeitado por 12 votos favoráveis, 01 voto contrário, 01 abstenção e 12 ausências. Em 2ª Discussão e Redação Final foram aprovados: 01) Projeto de Lei nº 084/17 que Dispõe sobre a criação do 'Dia da Troca de Livros' nas escolas do município e dá outras providências, de autoria do Vereador Wender Marques, aprovado por maioria simples simbólica; 02) Projeto de Lei nº 149/17 que Declara o Movimento Hip Hop Manifestação Cultural Popular no município de Uberlândia e dá outras providências, de autoria do Vereador Felipe Felps, aprovado por maioria simples simbólica; 03) Projeto de Lei nº 363/17 que Institui o Dia da Conscientização da Cardiopatia Congênita a ser realizado, anualmente no dia 12 de junho e dá outras providências, de autoria do Vereador Wilson Pinheiro, aprovado por maioria simples simbólica; 04) Projeto de Lei nº 364/17 que Inclui no calendário oficial do município de Uberlândia o "Dia Municipal do Advogado Criminalista", a ser comemorado no dia 02 de dezembro, de autoria dos Vereadores Thiago Fernandes e Hélio Ferraz – Baiano, aprovado por maioria simples simbólica. Atendendo ao requerimento nº 8108/17 do Vereador Alexandre Nogueira utilizou a tribuna o Deputado Estadual Dr. Arnaldo Silva Júnior, para fazer prestação de contas das atividades desenvolvidas no seu mandato parlamentar. Atendendo ao requerimento nº 8176/17 do Vereador Silésio Miranda utilizou a tribuna o Sr. Marden de Melo Morais, representando o Conselho de Pais da EMEI Irmã Aparecida Monteiro. O 1º Vice-Presidente, Wilson Pinheiro, encerrou a presente reunião às 11h42m por falta de quórum, da qual mandou lavrar esta ata que, depois de lida e aprovada, será por mim assinada e transcrita nos anais da Câmara Municipal, em resumo.

WILSON PINHEIRO
1º Vice-Presidente
JULIANO MODESTO
1º Secretário

CONTROLE INTERNO

INSTRUÇÃO DE CONTROLE – IC nº 001/2017

A Coordenadoria do Controle Interno, CONSIDERANDO a Portaria 301/2004, vem adotando um plano de organização com métodos e medidas de caráter preventivo e sistemático, para estimular o cumprimento das políticas administrativas prescritas, com enfoque nos resultados, no tocante às despesas com a atividade parlamentar, selos postais e impressos em geral, combustíveis e manutenção dos veículos cadastrados neste Órgão de Controle, e averiguar a exatidão e fidelidade dos atos, de modo a antecipar-se às possíveis ocorrências indesejáveis. No entanto, quando essas acontecem, o Controle deve identificar as causas das práticas irregulares, de modo a introduzir medidas que impeçam sua repetição.

A sua função é guiar e orientar os gestores e agentes políticos com vistas ao aperfeiçoamento de cada programa, projeto e

atividade, para que o resultado de cada atuação seja atingido de maneira eficaz.

Tem ainda o fim de corrigir os desperdícios, coibir a improbidade, a negligência e a omissão, mas, principalmente, antecipando-se a essas ocorrências e garantindo os resultados pretendidos pela Administração Pública. Diante disso, RESOLVE instituir a IC nº 001/2017 nos termos que se apresenta:

1. Quanto ao Informativo da Atividade Parlamentar:

1.1 A partir do presente mês, o layout (colorido) do Informativo Parlamentar deverá ser entregue à Coordenadoria do Controle Interno, no máximo em três dias úteis que antecedam o encerramento de cada mês, para devida apreciação pela equipe e posterior aprovação pelo Controlador. Com este procedimento poderemos fazer análise crítica dentro dos parâmetros já estabelecidos, com prazo para eventuais correções e emissão da nota fiscal. Reiteramos que, os exemplares apresentados para análise fora do prazo estabelecido serão terminantemente recusados e eventual confecção por parte do Gabinete neste caso, será avaliada na ocasião da apresentação da Verba Indenizatória, podendo ser aprovado ou reprovado o Informativo, e neste segundo caso será indeferida a indenização.

1.2 As gráficas responsáveis pela impressão e criação dos informativos deverão estar aptas para tal serviço, comprovadas pelo registro do CNAE - Classificação Nacional de Atividades Econômicas, estabelecido pela Receita Federal e com a situação regular perante o fisco em geral. A quitação na NF com o carimbo de "recebemos" deverá constar o razão social da empresa e estar assinada por extenso, sendo vedada rubrica e ainda devidamente datada.

1.3 A não observância da exigência estabelecida no item 1.2 com as Notas Fiscais acarretará a não indenização da referida despesa. Recomendamos ao responsável pela verba indenizatória, tomar as providências cabíveis antes de efetivada a contratação dos serviços.

1.4 Caso o informativo apresente imagens/fotos correlatas aos textos, estas deverão conter suas "fontes" quer seja individualmente ou no rodapé do exemplar.

1.5 A expressão "apoio" ou expressões similares, em participações do parlamentar nas festividades e eventos, indicam em geral atividade fora do contexto parlamentar, pelo que não serão acatadas na avaliação, haja vista que, em geral, remete a promoção pessoal. Ressalta-se que estes deverão ser de caráter exclusivamente educativo, de orientação social e informativo, conforme Instrução Normativa nº 01/1992 do TCE/MG.

1.6 As duas amostras finais anexadas à Nota Fiscal para pedido de indenização devem contemplar todas as recomendações/orientações/correções que foram feitas no Controle de Avaliação do Informativo Parlamentar, emitido por esta CCI, estejam em 1ª, 2ª ou 3ª avaliação. Este formulário, com todas as avaliações que se fizeram necessárias, também acompanha o pedido de indenização.

2. Quanto à distribuição do Informativo da Atividade Parlamentar:

2.1 Fica estabelecido até o dia 15 ou dia útil seguinte, do mês subsequente à impressão do informativo, a entrega do Relatório de Distribuição do Informativo na CCI anexando as fotos comprobatórias da entrega, e contendo o período, os nomes dos assessores que procederam a entrega e os bairros contemplados pela distribuição. Estão dispensados da entrega apenas aqueles que utilizarem mala direta via EBCT - Correios, para a distribuição dos exemplares, comprovado mediante o pedido de indenização e entrega do cupom fiscal da Agência dos Correios.

3. Quanto à entrega do RAQ – RELATÓRIO DE ACOMPANHAMENTO DE QUILOMETRAGEM:

3.1 O prazo máximo de entrega do RAQ na Seção de Almoxarifado e Patrimônio é o dia 05 ou dia útil seguinte, do mês subsequente ao abastecimento, assinado pelo vereador ou chefe de gabinete, sempre acompanhado dos cupons fiscais originais com todas as informações pertinentes e do relatório dos veículos cadastrados como Bens de Terceiros emitido pelo Sistema. Na sua falta o Gabinete se sujeita a notificação e ou ao bloqueio do abastecimento no mês corrente, após este prazo.

3.2 Caso seja solicitado pela equipe da CCI alguma correção no RAQ, o responsável terá o prazo de 48 horas a partir da notificação, para as devidas correções e nova apresentação na CCI.

3.3 Se porventura ocorrer abastecimento excedente ao limitado pela CCI, este ocorrerá às expensas do Parlamentar com pagamento direto ao Contratado.

4. Quanto aos veículos cadastrados na CCI:

4.1 É obrigatório manter atualizado o CRLV (Certificado de Registro e Licenciamento de Veículo) do veículo cadastrado na CCI, para manutenção e abastecimento com recursos públicos, assim deverá o responsável apresentar a cópia legível do documento, impreterivelmente até 31/08 de cada exercício na CCI.

4.2 Caso ocorra o descumprimento do item 4.1, ficará a critério do Controlador analisar a questão e determinar ou não o descadastramento do veículo que esteja irregular com o CTB e as normas complementares, estando este, portanto, desautorizado a efetuar qualquer despesa no veículo.

4.3 Os veículos cadastrados na CCI para abastecimento e manutenção por meio de recursos públicos, não poderão ser repassados a terceiros sem prévia análise da equipe da CCI, em especial aqueles que realizarem manutenção, cujo descadastramento somente poderá ocorrer, após 06 (seis) meses contados da última manutenção - Portaria 376/2011. Ademais estes veículos não poderão conter plotagem e propaganda de qualquer espécie.

4.4 As notas fiscais decorrentes das despesas com manutenção dos veículos cadastrados na CCI deverão ser entregues ao Diretor Administrativo desta Casa Legislativa.

Consigne-se que os atos administrativos realizados sem a observância, do disposto acima, podem ser considerados irregulares, sujeitando, portanto, ao ressarcimento ao erário público.

Fica ratificada a aplicabilidade de todas as instruções e memorandos estabelecidos por esta Controladoria, que deverá ser seguido rigorosamente pelo responsável da atividade parlamentar com orientações e conferência da equipe da CCI, que tem como função importante a de auxiliar o gestor público na elaboração de uma apropriada prestação de contas, uma vez que, na Administração Pública, todos os que guardam e administram bens ou recursos têm o dever de prestar contas.

Demais situações não previstas nesta instrução serão avaliadas, dentre outras, em consonância com a legislação, consultas respondidas pelo TCE, manifestações do MPE e da Procuradoria da Casa.

A Coordenadoria do Controle Interno se reserva o direito de alterar ou revogar total ou parcialmente esta instrução, a qualquer tempo e em conformidade com as diretrizes legais.

Esta Instrução de Controle entra em vigor a partir da sua assinatura.

Uberlândia, 17 de agosto de 2017.

Prof. Dr. Adeilson Barbosa Soares
Coordenador do Controle Interno

O LEGISLATIVO ANO XV Nº 2191, SEXTA-FEIRA, 18 DE AGOSTO DE 2017
EDIÇÃO DE HOJE 05 PÁGINAS - ÓRGÃO OFICIAL DA CÂMARA MUNICIPAL DE UBERLÂNDIA/MG CRIADO PELA LEI MUNICIPAL Nº 8485 DE 24/11/2003. AV. JOÃO NAVES DE ÁVILA, 1617 | 38408-414 | (34) 3239-1130 - EDITADO E PRODUZIDO PELA DIRETORIA DE COMUNICAÇÃO/SEÇÃO DE JORNALISMO COM BASE NA DOCUMENTAÇÃO DISPONIBILIZADA PELOS DEPARTAMENTOS. DIRETOR DE COMUNICAÇÃO: **ADEMIR REIS (MG04854JP)**; CHEFE DA SEÇÃO DE JORNALISMO: **PEDRO JORGE DOS REIS MG07436JP**; JORNALISTA RESPONSÁVEL: **EITHEL LOBIANCO JR. 3484 MTE/SJPMG**; EDITORAÇÃO ELETRÔNICA: SEÇÃO DE JORNALISMO. PUBLICIZADO NO SITE DA CÂMARA: **WWW.CAMARAUBERLANDIA.MG.GOV.BR** E DISPONIBILIZADO NA REDE INTERNA PARA DEPARTAMENTOS E GABINETES DOS VEREADORES. EDIÇÕES ANTERIORES SOLICITE PELO E-MAIL: **IMPRENSA@CAMARAUBERLANDIA.MG.GOV.BR**