CNPJ sob nº 03.088.280/0001-20, neste ato representada pela Secretária Municipal de Educação, Sra. Maria Loureto de Lima, devidamente constituída por Portaria nº 1082/2017.

CONTRATADA:

EMPRESA JOSINEIDE MORAIS TRIBUTINO-ME, pessoa jurídica de direito privado, com endereço na Rua do Cruzeiro, nº 761, São Miguel, em Juazeiro do Norte, Estado do Ceará, inscrita no CNPJ sob nº 09.342.699/001-42.

Aos 06 (seis) dias do mês de outubro do ano de dois mil e dezessete (2017), na sede da Secretaria de Educação do Município de Juazeiro do Norte, a parte acima qualificada, denominada CONTRATANTE, faz RESCINDIR UNILATERALMENTE o Contrato Administrativo Nº 2017.04.12.03/SEDUC, nos termos e condições expressos na cláusula que segue:

CLÁUSULA PRIMEIRA - Fica, a partir da presente data, RESCINDIDO o Contrato Administrativo Nº 2017.04.12.03/SEDUC, que tem como objeto a aquisição de gêneros alimentícios perecíveis para compor a merenda escolar destinada às escolas da rede pública municipal de ensino.

Publique-se e cumpra-se.

Juazeiro do Norte/CE, 06 de outubro de 2017

MARIA LOURETO DE LIMA

Secretária de Educação

Portaria nº. 1082/2017

TERMO DE RESCISÃO CONTRATUAL

TERMO DE RESCISÃO UNILATERAL DO CONTRATO ADMINISTRATIVO Nº 2017.03.21.05/SEDUC, CELEBRADO ENTRE O MUNICÍPIO DE JUAZEIRO DO NORTE, POR INTERMÉDIO DA SECRETARIA MUNICIPAL DE EDUCAÇÃO, E EMPRESA JOSINEIDE MORAIS TRIBUTINO-ME.

CONTRATANTE:

O MUNICÍPIO DE JUAZEIRO DO NORTE-CE, por intermédio da SECRETARIA MUNICIPAL DE EDUCAÇÃO, pessoa jurídica de direito público interno, com sede na Rua 15 de Novembro, s/n, São Miguel, em Juazeiro do Norte, Estado do Ceará, inscrita no CNPJ sob nº 03.088.280/0001-20, neste ato representada pela Secretária Municipal de Educação, Sra. Maria Loureto de Lima, devidamente constituída por Portaria nº 1082/2017.

CONTRATADA:

EMPRESA JOSINEIDE MORAIS TRIBUTINO-ME, pessoa jurídica de direito privado, com endereço na Rua do Cruzeiro, nº 761, São Miguel, em Juazeiro do Norte, Estado do Ceará, inscrita no CNPJ sob nº 09.342.699/001-42.

Aos 06 (seis) dias do mês de outubro do ano de dois mil e dezessete (2017), na sede da Secretaria de Educação do Município de Juazeiro do Norte, a parte acima qualificada, denominada CONTRATANTE, faz RESCINDIR UNILATERALMENTE o Contrato Administrativo nº 2017.03.21.05/SEDUC, nos termos e condições expressos na cláusula que segue:

CLÁUSULA PRIMEIRA - Fica, a partir da presente data, RESCINDIDO o Contrato Administrativo Nº 2017.03.21.05/SEDUC, que tem como objeto a aquisição de gêneros alimentícios para compor a merenda escolar destinada às escolas da rede pública municipal de ensino.

Publique-se e cumpra-se.

Juazeiro do Norte/CE, 06 de outubro de 2017

MARIA LOURETO DE LIMA

Secretária de Educação

Portaria nº. 1082/2017

PREVIJUNO

Portaria Administrativa nº 002/2017

DISPÕE SOBRE A POLITICA DE SEGURANÇA DAS INFORMAÇÕES-PSI E AS ADEQUAÇÕES DA PSI DO PREVIJUNO

A Gestora do Fundo Municipal de Previdência Social dos Servidores de Juazeiro do Norte – CE – PREVIJUNO - MARIA DAS GRAÇAS ALVES SILVA, brasileira, gestora, com endereço funcional na sede do PREVIJUNO, conforme nomeação efetuada pela portaria nº 1098/2017, nos exatos termos das atribuições previstas na Lei Complementar Municipal Nº 25, de 8 de Junho de 2007, anexo II, 1, I e outras, vem editar e dar conhecimento da

portaria epigrafada para os fins previstos em lei e pelo melhor interesse administrativo deste Fundo,

CONSIDERANDO QUE A informação é um ativo que deve ser protegido e cuidado por meio de regras e procedimentos das políticas de segurança, do mesmo modo que protegemos nossos recursos financeiros e patrimoniais;

CONSIDERANDO QUE a politica de segurança deve iniciar com o fortalecimento da cultura de proteção a informações;

CONSIDERANDO QUE uma política de segurança é um instrumento importante para proteger a sua organização contra ameaças à segurança da informação que a ela pertence ou que está sob sua responsabilidade. Uma ameaça à segurança é compreendida neste contexto como a quebra de uma ou mais de suas três propriedades fundamentais (confidencialidade, integridade e disponibilidade).

CONSIDERANDO QUE Desta forma, elas sabem quais as expectativas que podem ter e quais são as suas atribuições em relação à segurança dos recursos computacionais com os quais trabalham. Além disso, a política de segurança também estipula as penalidades às quais estão sujeitos aqueles que a descumprem.

CONSIDERANDO QUE O PREVIJUNO armazena informações cadastrais, funcionais e financeiras dos servidores segurados obrigatórios do RPPS de Juazeiro do Norte – CE, de seus próprios funcionários, resolve através da presente PORTARIA, prover e dar conhecimento a todos os servidores do PREVIJUNO, as regras que se segue:

CAPÍTULO I DOS FUNDAMENTOS

Art. 1º - Um sistema de segurança da informação baseia-se em três princípios básicos:

a) Confidencialidade,

b) Integridade e

c) Disponibilidade.

§ 1º - Se falar em segurança da informação, deve-se levar em consideração estes três princípios básicos, pois toda ação que venha a comprometer qualquer um desses princípios, atentará contra a sua segurança.

§ 2º - Confidencialidade: A confidencialidade é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso. Caso a informação seja acessada por uma pessoa não autorizada, intencionalmente ou não, ocorre a quebra da confidencialidade. A quebra desse sigilo pode acarretar danos inestimáveis para a empresa ou até mesmo para uma pessoa física.

§ 3º - Integridade: A integridade é a garantia da exatidão e completeza da informação e dos métodos de processamento. Garantir a integridade é não permitir que a informação seja modificada, alterada ou destruída sem autorização; que ela seja legítima e permaneça consistente. Quando a informação é alterada, falsificada ou furtada, ocorre à quebra da integridade. A integridade é garantida quando se mantém a informação no seu formato original.

§ 4º - Disponibilidade: A disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. Quando a informação está indisponível para o acesso, ou seja, quando os servidores estão inoperantes por conta de ataques e invasões, considera-se um incidente de segurança da informação por quebra de disponibilidade. Mesmo as interrupções involuntárias de sistemas, ou seja, não intencionais, configuram quebra de disponibilidade.

Art. 2º - Sobre o SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI) devem-se obedecer as seguintes normas de Política de Segurança da Informação;

a) Organização da segurança da informação;

b) Gestão de ativos;

c) Segurança em recursos humanos;

d) Segurança física e do ambiente;

e) Gestão das operações e comunicações;

f) Controle de acesso;

g) Aquisição, desenvolvimento e manutenção de sistemas de informação;

h) Gestão de incidentes de segurança da informação;

i) Gestão da continuidade do negócio e conformidade;

j) Sigilo sobre as informações acessadas pelos integrantes do PREVIJUNO.

Parágrafo único - O sistema de gestão de segurança da informação é o resultado da sua aplicação planejada, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que, de forma conjunta, definem como são reduzidos os riscos para a segurança da informação.

Art. 3º - CLASSIFICANDO AS INFORMAÇÕES

a) A principal razão em classificar as informações, é de que elas não possuem o mesmo grau de confidencialidade, ou então as pessoas podem ter interpretações diferentes sobre o nível de confidencialidade da informação.

b) Antes de se iniciar o processo de classificação é necessário conhecer o processo de negócio da organização, compreender as atividades realizadas e, a partir disso, iniciar as respectivas classificações.

c) As informações podem ser classificadas em informações públicas, quando não necessita de sigilo algum; informações internas, quando o acesso externo as informações deve, ser negado; e informações confidenciais, quando essas devem ser confidenciais tanto dentro da empresa quanto fora dela e protegidas contra tentativas de acesso interno e/ou externo.

ES:Art. 4º - A definição clássica é que o ativo compreende ao conjunto de bens e direitos de uma entidade. Entretanto, atualmente, um conceito mais amplo tem sido adotado para se referir ao ativo como tudo aquilo que possui valor para a empresa.

Parágrafo único - A informação ocupa um papel de destaque no ambiente das organizações empresariais, e também adquire um potencial de valorização para as empresas e para as pessoas, passando a ser considerado o seu principal ativo.

Art. 5º - A ameaça pode ser considerada um agente externo ao ativo de informação, pois se aproveita de suas vulnerabilidades para quebrar um ou mais dos princípios básicos da segurança da informação – a confidencialidade, integridade e/ou disponibilidade.

Parágrafo único - As ameaças podem ser divididas em dois tipos básicos: As naturais - são aquelas que se originam de fenômenos da natureza; As involuntárias - são as que resultam de ações desprovidas de intenção para causar algum dano, e; As intencionais - são aquelas deliberadas, que objetivam causar danos, tais como às realizadas pelos hackers ou crackers.

Art. 6º - A vulnerabilidade é definida como uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Vulnerabilidade são as fraquezas presentes nos ativos, que podem ser exploradas, seja ela intencionalmente ou não, resultando assim na quebra de um ou mais princípios da segurança da informação.

§ 1º - Após terem sido identificadas as vulnerabilidades ou os pontos fracos, é possível dimensionar os riscos ao qual o ambiente está exposto e assim definir medidas de segurança apropriadas para sua correção.

§ 2º - As vulnerabilidades podem advir de vários aspectos: instalações físicas desprotegidas contra incêndios, inundações, e desastres naturais; material inadequado empregado nas construções; ausência de política de segurança para RH; funcionários sem treinamento e/ou locais de trabalho insatisfatórios; ausência ou não utilização de procedimento de controle de acesso e/ou utilização de equipamentos por pessoal contratado sem a observância dos requisitos citados anteriormente ou desautorizados; equipamentos obsoletos, sem manutenção e sem restrições para sua utilização; além de softwares sem patch de atualização e/ou sem licença de funcionamento.

Art. 7º - Com relação à segurança, os riscos são compreendidos como condições que criam ou aumentam os potenciais de danos e perdas. É medido pela possibilidade de um evento vir a acontecer e produzir perdas.

Art. 8º - Para evitar possíveis perdas de informações, que dependendo do seu grau de sigilo, poderá levar a empresa a problemas graves, é necessária a elaboração de uma gestão de riscos, onde os riscos são determinados e classificados, sendo depois realizado um conjunto equilibrado de medidas de segurança que permitirá reduzir ou eliminá-los a que o órgão possa estar sujeito além de garantir melhor eficiência nas ações preventivas.

Art. 9º - O backup dos sistemas deve ser armazenado periodicamente em outra mídia, e guardado o mais longe possível do ambiente atual, como em outro setor (cofre da instituição, por exemplo). O procedimento de backup é um dos recursos mais efetivos para assegurar a continuidade das operações em caso de paralisação por conta da ocorrência de algum sinistro.

*Art. 10 - Convém que sejam utilizados perímetros de segurança para proteger as áreas que contenham informações e instalações de processamento da informação.

*Art. 11 - Apesar de todos os cuidados em se definir os perímetros de segurança, essa ação não produzirá resultados positivos se os colaboradores não estiverem sintonizados com a cultura de segurança da informação. Essa cultura deve estar pulverizada em todo o órgão e especialmente consolidada dentro das áreas críticas de segurança. A informação pertinente ao trabalho dentro dessas áreas deve estar restrita a própria área e somente durante a execução das atividades em que ela se torna necessária.

Parágrafo único - Os locais escolhidos para a instalação dos equipamentos devem estar em boas condições de uso, com boas instalações elétricas, devem conter extintores de incêndios, bem como preferencialmente saídas de emergência, alarme contra incêndio, entre outros aspectos que devem ser levados em consideração.

CAPÍTULO II DOS ATOS NORMATIVOS

Art. 12 - A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI pode-se definir como um documento que

estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades sobre o que deve ser feito para alcançar um padrão desejável de proteção para as informações.

§ 1º - Ela é basicamente um manual de procedimentos que descreve como os recursos de TI da empresa devem ser protegidos e utilizados e é o pilar da eficácia da segurança da informação. Sem regras pré-estabelecidas, ela torna-se inconsistentes e vulnerabilidades podem surgir.

§ 2º - A política tende a estabelecer regras e normas de conduta com o objetivo de diminuir a probabilidade da ocorrência de incidentes que provoquem, por exemplo, a indisponibilidade do serviço, furto ou até mesmo a perda de informações.

§ 3º - As políticas de segurança geralmente são construídas a partir das necessidades do negócio e eventualmente aperfeiçoadas pela experiência do gestor.

§ 4º - O intervalo médio utilizado para a revisão da política é de seis meses ou um ano, porém, deve ser realizada uma revisão sempre que forem identificados fatos novos, não previstos na versão atual que possam ter impacto na segurança das informações da organização.

§ 5º - É recomendado que a política de segurança da informação seja revisada periodicamente e de forma planejada ou quando ocorrerem mudanças significativas, para assegurar a sua continua pertinência, adequação e eficácia.

§6º -A política de segurança não define só procedimentos específicos de manipulação e proteção da informação, mas atribui direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas e funcionários) que lidam com essa informação.

Art. 13 - A política de segurança da informação deve estabelecer:

§ 1º - Como será efetuado o acesso às informações de todas as formas possíveis, seja ela internamente ou externamente;

§ 2º - Quais os tipos de mídias poderão transportar e ter acesso a esta informação.

§ 3º - A política deve especificar os mecanismos através dos quais estes requisitos podem ser alocados.

CAPÍTULO III DA ORGANIZAÇÃO E DO CUMPRIMENTO

Art. 14 - A política de segurança da informação do PREVIJUNO comporá de um gestor de área afins do município que tenha responsabilidade de gestão.

§ 1º - A responsabilidade das informações do PREVIJUNO está com a Secretaria de Administração e Finanças devido esta Unidade Gestora ainda ser vinculada a administração direta, ressaltando que as informações deverão serem armazenadas em servidores de redes exclusivos do PREVIJUNO.

§ 2º - Os servidores de redes do PREVIJUNO atualmente são feitos por computadores/desktops que executam essa função e deverão encontrar-se na sede do instituto para condicionamento das informações exclusivas do mesmo.

§ 3º - No cenário atual, em que as empresas dependem cada vez mais da tecnologia e da informação - TI, é vital garantir a segurança adequada deste ativo, considerado estratégico em sua missão de prestar serviços de qualidade.

§ 4º - O conjunto de normas e regras que regulem a utilização dos sistemas das empresas, assim como o acesso a redes sociais e e-mails pessoais.

§ 5º - Também é importante lembrar que os servidores devem estar cientes do monitoramento.

Art. 15 - A política de segurança da informação do PREVIJUNO estende também à empresa terceirizada onde mantêm o site www.previjuno.com, os serviços on-line, aplicativos administrativos e os e-mails institucionais, onde tem regras específicas, porém que atendem a politica de segurança de informação da contratada.

Art. 16 - Quando necessário será contratada empresa especializada para estudo das vulnerabilidades e se existir será realizado ações para saná-las.

Art. 17 - Quando da necessidade de cadastramento de um novo usuário para utilização do SISPREVWEB, ou outros sistemas ou equipamentos de informática no PREVIJUNO, o setor de origem do novo usuário deverá comunicar esta necessidade ao setor de Informática (TI) por meio de memorando, e-mail ou correio interno, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

Art. 18 - É terminantemente proibido o uso de programas ilegais (PIRATAS) e/ou desautorizados pelo Setor de Informática (TI). Os usuários não podem, em hipótese alguma, instalar este tipo de "software" (programa) nos equipamentos/computadores e afins. Periodicamente, o Setor de Informática (TI) fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz.

Art. 19 - O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva do Setor de Informática (TI), assim como a manutenção, alteração e atualização de equipamentos e programas.

Art. 20 aç:– A Direção administrativa deverá informar ao setor de Informática, toda e qualquer movimentação de temporários e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou excluídos no sistema do Órgão. Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema (user-id), pelo Setor de Informática (TI).

Art. 21 - É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de textos, planilhas, mensagens eletrônicas, desenhos e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios do PREVIJUNO.

Art. 22 - É de propriedade do PREVIJUNO, todos os "designs", criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício.

CAPÍTULO IV

DO ACESSO E DAS PROIBIÇÕES

Art. 23 - O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o desenvolvimento do trabalho não devem ser acessados.

§ 1º - O uso da Internet será monitorado pelo Setor de Informática (TI), inclusive através de "logs" (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

§ 2º - A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição da gestora do PREVIJUNO ou responsável definido pela mesma, com base, também, em recomendação do Setor de Informática (TI).

§ 3º - Não é permitido instalar programas provenientes da Internet nos microcomputadores do órgão, sem expressa anuência do setor de Informática (TI), exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais, todos previamente informados ao Setor de Informática (TI).

§ 4º - Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

§ 5º - Quando navegando na Internet, é proibido a visualização, transferência (downloads/uploads), cópia ou qualquer outro tipo de acesso a sites:

a) De estações de rádio;

b) De conteúdos pornográficos ou relacionados a sexo;

c) Que defendam atividades ilegais;

d) Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;

e) Que promovam a participação em salas de discussão de assuntos não relacionados aos serviços;

f) Que promovam discussão pública sobre os assuntos do órgão, a menos que autorizado pela Diretoria;

g) Que possibilitem a distribuição de informações de níveis "Confidenciais".

h) Que permitam a transferência (downloads ou uploads) de arquivos e/ou programas ilegais.

i) Que permitem a transferência (downloads ou uploads) de arquivos e/ou programas que promovam o acesso remoto a qualquer dispositivo do PREVIJUNO, sem a anuência do Setor de Informática (TI).

j) Que permitam a transferência (downloads ou uploads) de arquivos e/ou programas que busquem na rede interna e/ou externa vulnerabilidades em dispositivos e/ou serviços de qualquer natureza , salvo em casos de anuência da gestora e/ou Setor de Informática (TI).

k) Que permitam o uso e/ou armazenamento de programas e/ou serviços relacionados a entretenimento tais como jogos, karaokê e desafios (ou similares).

l) Será disponibilizado um servidor de arquivos, contendo diretórios para cada setor do PREVIJUNO onde os funcionários lotados no setor especifico terão acesso, e ainda será disponibilizado acesso comum a setores distintos e/ou a todos os setores quando os dados constantes nos diretórios subsidiar o desenvolvimento do trabalho da Instituição em mais de um setor, assim será cognominado o diretório de "PublicoNet".

m) A Diretoria do PREVIJUNO na pessoa do gestor terá acesso a todos os diretórios da Instituição.

Art. 24 - O correio eletrônico fornecido pelo PREVIJUNO é um instrumento de comunicação interna e externa para a realização do negócio do Órgão.

§ 1º - As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem do PREVIJUNO, não podem ser contrárias à legislação vigente e nem aos princípios éticos do PREVIJUNO.

§ 2º - O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.

Art. 25 - É terminantemente proibido o envio de mensagens que:

a) Contenham declarações difamatórias e linguagem ofensiva;

b) Possam trazer prejuízos a outras pessoas;

c) Sejam hostis e inúteis;

d) Sejam relativas a "correntes", de conteúdos inúteis, pornográficos ou equivalentes;

e) Possam prejudicar a imagem da organização;

f) Possam prejudicar a imagem de outras empresas;

g) Sejam incoerentes com as políticas do PREVIJUNO.

§ 1º - Para incluir um novo usuário no correio eletrônico, a Diretoria deverá fazer um pedido formal ao Setor de Informática, que providenciará a inclusão do mesmo.

§ 2º - A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado. Em caso de congestionamento no Sistema de correio eletrônico o Setor de Informática fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo.

Art. 26 - O Setor de Informática é responsável pela aplicação da Política do órgão em relação à compra e substituição de "software" e "hardware".

Parágrafo único - Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pelo setor de Informática.

Art. 27 - Os usuários que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade do PREVIJUNO, devem estar cientes de que:

§ 1º - Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo realização de atividades profissionais.

§ 2º - A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.

§ 3º - É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.

§ 4º - O usuário não deve alterar a configuração do equipamento recebido.

Art. 28 - Alguns cuidados que devem ser observados:

§ 1º - Fora do trabalho:

a) Mantenha o equipamento sempre com você;

b) Atenção em hall de hotéis, aeroportos, aviões, táxi, etc.;

c) Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível;

d) Atenção ao transportar o equipamento na rua.

§ 2º - Em caso de furto:

a) Registre a ocorrência em uma delegacia de polícia;

b) Comunique ao seu superior imediato e ao Setor de Informática;

c) Envie uma cópia da ocorrência para o Setor de Informática.

Art. 29 - Os responsáveis pelos setores são responsáveis pelas definições dos direitos de acesso de seus funcionários aos sistemas e informações, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

§1º - O Setor de verificará se houve acesso dos usuários às informações, verificando:

a) Que tipo de informação o usuário pode acessar;

b) Quem está autorizado a acessar determinada rotina e/ou informação;

a. Quem acessou determinada rotina e informação;

b. Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;

c. Que informação ou rotina determinado usuário acessou;

d. Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

e. Se algum usuário teve acesso de forma indevida a senhas de sistemas do CADPREV, BANCOS, E-MAIL e/ou tipos de sistemas.

§2º - O exercício fiscalizatório acima previsto deverá ser exercido com moderação e estrita observância da necessidade de forma a não implicar em violação de intimidade de qualquer servidor ou de seus dados eletrônicos por parte do servidor, implicara em cometimento de crime previsto na LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012, que trata sobre a tipificação criminal de delitos informáticos, com possibilidade de Ação penal incondicionada, prescindindo de representação por parte do ofendido.

§3º - Todas as informações e dados colhidos no âmbito do PREVIJUNO no exercício do poder fiscalizatório enumerado no parágrafo 1º é integralmente sigilosa, não podendo ser exposta a terceiro, devendo constar unicamente em relatório técnico que deve ser entregue diretamente à Gestão do PREVIJUNO, para adoção das medidas cabíveis;

§4º - Todos os funcionários que tenham acesso às informações de qualquer natureza, seja de processos eletrônicos ou físicos, dados eletrônicos e pessoais de segurados e funcionários do PREVIJUNO, encontra-se vinculado a dever de sigilo profissional art. 154 do Código Penal e abrangido por obrigação civil de não fazer, sujeitando-se às penalidades previstas no art. 251 do Código Civil.

§5º - todos os dados que o setor de Tecnologia da Informação armazenar em dispositivos como pendrive, HD externo ou similar, por motivo de transferência de dados das máquinas, entre outros, deverão ser posteriormente excluídos de tais dispositivos com total segurança.

§6º - Deverá o setor de TI ter uma rotina de verificação de máquinas e equipamentos de informática nos setores, recebendo a demanda dos usuários e realizando o atendimento.

Art. 30 - Todo arquivo em mídia proveniente de entidade externa ao órgão deve ser verificado por programa antivírus.

§ 1º - Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus.

§ 2º - Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Informática, via rede.

§ 3º - O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

Art. 31 – Quanto aos equipamentos e informações contidas nos mesmos:

a) É proibida a execução de programas botáveis nos computadores e/ou equipamentos do PREVIJUNO sem o devido consentimento da gestora e/ou setor de informática.

b) É proibido abrir quaisquer equipamentos relacionados à área de informática (ou similares) com o intuito de realizar reparos, troca de peças, instalação de novos dispositivos ou complementos (físicos e/ou virtuais) sem o devido consentimento da gestora e/ou setor de informática.

c) Tornar ciente de que o PREVIJUNO não é responsável por informações pessoais que não se referem à natureza de sua operação, definindo essas informações como sendo indevidas para uso interno à instituição.

d) É terminantemente proibido disseminar, intencional ou não, vírus ou qualquer programa que gere ameaça à continuidade do serviço.

e) É proibido o compartilhamento de senhas e/ou similares, sendo o usuário responsabilizado pelo seu uso indevido.

Art. 32 en:–É proibido o uso de notebook ou similares, de propriedade privada dos funcionários do PREVIJUNO, para uso no desenvolvimento de trabalhos da instituição e também de arquivamento de dados, sejam imagens, textos ou quaisquer dados exclusivo da Instituição;

Art. 33 – Quando empresa contratada para prestação de serviços no PREVIJUNO solicitar arquivos, banco de dados ou similares, o setor de TI só fornecerá mediante autorização do gestor.

CAPÍTULO V DO CUMPRIMENTO DAS ORIENTAÇÕES

Art. 34 - O não cumprimento da Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, e exoneração do cargo.

§ 1º - Respeitar-se-á a Lei 12, de 17 de agosto de 2006 – Estatuto dos Servidores Públicos no que se refere ao Regime Disciplinar.

§ 2º - No que couber, outra ação disciplinar e/ou processo civil ou criminal dependendo da gravidade.

Publique-se e arquive-se.

Juazeiro do Norte, 19 de Outubro de 2017.

MARIA DAS GRAÇAS ALVES SILVA

GESTORA – PREVIJUNO

Portaria Nº 1098/2017

AVISOS E EDITAIS

AVISO

CONCORRÊNCIA PÚBLICA NACIONAL N°. 04/2017-SESAU

Pelo presente aviso e em cumprimento à Lei n°. 8.666/93 e suas alterações, o Governo Municipal de Juazeiro do Norte, Ceará, comunica aos interessados que realizará no dia 22/11/2017, às 09h (Horário de Brasília), no Palácio Municipal José Geraldo da Cruz – Praça Dirceu Figueiredo, s/nº - Centro – CEP: 63010-010, Juazeiro do Norte, Ceará, na Sala da Comissão Permanente de Licitação a Concorrência Pública Nacional n°. 04/2017-SESAU para contratação de empresa para construção de um sistema de esgotamento sanitário do Centro de Reabilitação e da Oficina Ortopédica no Município de Juazeiro do Norte, Ceará, Conforme PT nº 0389531-35. Edital e demais informações poderão ser adquiridas no endereço supramencionado, de segunda a sexta-feira, de 08h às 12h e de 14h às 17h. Juazeiro do Norte, Ceará 19 de outubro de 2017. José Wilson Marques Júnior - Presidente da Comissão Permanente de Licitação do Município de Juazeiro do Norte, Ceará.

EXTRATO DO CONTRATO

Extrato de Contrato nº 2017.10.11.16/SEDUC. Partes: O Município de Juazeiro do Norte/CE, por intermédio da Secretaria de Educação e a empresa JOSIMAR ARAUJO DE SOUZA - ME. Objeto: Aquisições de materiais e serviços gráficos para atender as necessidades das escolas da rede pública municipal e da sede da Secretaria de Educação do Município de Juazeiro do Norte/Ce. Valor R$ 2.627,50 (dois mil, seiscentos e vinte e sete reais e cinquenta centavos). Pregão Eletrônico n° 06/2017-SEDUC. Prazo Vigência do Contrato: 11/10/2017 a 31/12/2017. Signatários: Maria Loureto de Lima e Pedro Almeida Custodio.

EXTRATO DO CONTRATO

Extrato de Contrato Nº 2017.10.16.01-SESAU. Partes: O Município de Juazeiro do Norte/CE, por intermédio da Secretaria de Saúde e a outro LOCMED Hospitalar LTDA. Objeto: locações de equipamentos hospitalares para atendimentos das necessidades da Secretaria de Saúde do município de Juazeiro do Norte, Ceará. Valor de R$ 448.447,80 (quatrocentos e quarenta e oito mil, quatrocentos e quarenta e sete reais e oitenta centavos). Pregão Eletrônico nº 07/2017. Prazo Vigência do Contrato: 31/12/17.Juazeiro do Norte/CE, 16 de outubro de 2017. Signatários: Maria Nizete Tavares Alves e Emerson Pereira da Silva.

Extrato de Contrato nº 2017.10.18.02/SEDEST. Partes: o Município de Juazeiro do Norte/CE, por intermédio da Secretaria de Desenvolvimento Social e a empresa Eder Pereira Correia - ME. Objeto: Aquisição de Gêneros Alimentícios para atender as necessidades dos diversos setores da Secretaria de Desenvolvimento Social e Trabalho. Valor: R$ 623.261,08 (Seiscentos e Vinte e Três Mil, Duzentos e Sessenta e Oito Centavos). Prazo: 31/12/2017. Juazeiro do Norte/Ce., 18 de outubro de 2017. Signatários: Isabela Geromel Bezerra de Menezes e Eder Pereira Correia.

Extrato de Contrato nº 2017.10.18.03/SEDEST. Partes: o Município de Juazeiro do Norte/CE, por intermédio da Secretaria de Desenvolvimento Social e a empresa DS Andrade - ME. Objeto: Aquisição de Gêneros Alimentícios para atender as necessidades dos diversos setores da Secretaria de Desenvolvimento Social e Trabalho. Valor: R$ 540.053,84 (Quinhentos e Quarenta Mil, Cinquenta e Três Reais e Oitenta e Quatro Centavos). Prazo: 31/12/2017. Juazeiro do Norte/Ce., 18 de outubro de 2017. Signatários: Isabela Geromel Bezerra de Menezes e Diego Marcondes Cartaxo Tavares.

EXTRATO DA ATA DE REGISTRO DE PREÇOS

PREGÃO ELETRÔNICO Nº 27/2017-SESAU

Estado do Ceará - Prefeitura Municipal de Juazeiro do Norte - Extrato da Ata de Registro de Preços nº 27/2017-SESAU – Órgão Gerenciador: Secretaria de Saúde. Empresas Detentoras do Registro de Preços: Marinho Soares Comércio e Serviços LTDA-EPP, Lote 01, valor global R$ 92.249,40 e Lote 02, valor global R$ 58.604,00 e Pedro Renato de Aguiar de Melo –ME Lote 03, valor global R$ 395.773,40. Prazo: 12 (doze) meses a partir da assinatura da ata de registro de preço. Processo de licitação na modalidade Pregão Eletrônico para Registro de Preços nº 27/2017-SESAU. Objeto: Registro de preços visando a futura e eventual aquisição de equipamentos e suprimentos de informática junto a esta Secretaria de Saúde do Município de Juazeiro do Norte/CE. Signatários: Representante do Órgão Gerenciador: Secretaria de Saúde – Maria Nizete Tavares Alves. Representante da Empresa Detentora do Registro de Preços: Erivando Duarte Costa e Pedro Renato Aguiar de Melo. Data da assinatura: 10 de outubro de 2017.

AVISO ADIAMENTO DE LICITAÇÃO

CONCORRÊNCIA PÚBLICA NACIONAL N°. 03/2017 - SEMASP

O Presidente da Comissão Permanente de Licitação do Município de Juazeiro do Norte, Ceará, torna público para conhecimento dos interessados que a data de recebimento e abertura dos envelopes de Habilitação e Propostas de Preços da licitação na Modalidade Concorrência Pública Nacional N°. 03/2017 - SEMASP, cujo objeto é contratação de empresa especializada para os serviços de coleta de lixo hospitalar, resíduos infectantes grupo a (risco biológico) e grupo e (perfuro cortante) nos PSF'S, Hospitais, Centro de Dermatologia, Centro de Especialidades Odontológicas, Coordenação de Assistência Farmacêutica, Vigilância Sanitária, Centro de Zoonoses, CAPS Adulto e CAPS Infantil, Centro de Infectologia, foi adiada para o dia 30 de outubro de 2017, às 09:00 (Horário de Brasília), José Wilson Marques Junior – Presidente da Comissão Permanente de Licitação, 20 de outubro de 2017.