AGERSA

EXTRATO DE TERMO DE APOSTILAMENTO AO CONTRATO

Espécie	1° Termo de Apostilamento ao Contrato Administrativo n° 07/2014
Contratante	AGERSA – Agência Municipal de Regulação de Serviços Públicos Delegados de Cachoeiro de Itapemirim
CNPJ Contratante	03.311.730/0001-00
Contratado	DATACI – Companhia de Tecnologia da Informação de Cachoeiro de Itapemirim
CNPJ Contratado	31.720.485/0001-11
Objeto	Reajustar o valor mensal do contrato de acordo com a aplicação do IPCA/IBGE acumulado no período de 12 meses anteriores ao vencimento contratual.
Do valor	Com o presente apostilamento o valor mensal do contrato após o reajuste passará de R$ 2.050,00 (dois mil e cinquenta reais) para R$ 2.245,95 (dois mil duzentos e quarenta e cinco reais e noventa e cinco centavos), perfazendo o valor anual do contrato de R$ 26.951,40 (vinte e seis mil novecentos e cinquenta e um reais e quarenta centavos)
Data de Assinatura	22/09/2015
Vigência do Contrato	48 (quarenta e oito meses) a contar do dia subsequente a publicação do resumo do Diário Oficial do Município
Signatários	Fernando Santos Moura (Diretor Presidente da AGERSA), Edmar Lyrio Temporim (Diretor Presidente da DATACI) e Carla da Costa Araujo (Diretora de Tecnologia de Gestão DATACI)
Ano Processo	2014
Nº Processo	1183746 (Protocolo AGERSA n°. 9790/2014)
Fundamento Legal	Lei 8.666/1993, artigos 24, VIII / XVI, 57, IV e 65 §8°

FERNANDO SANTOS MOURA
Diretor Presidente

EXTRATO DE TERMO ADITIVO DE CONTRATO

Espécie	1° Termo Aditivo ao Contrato Administrativo n° 06/2014
Contratante	AGERSA – Agência Municipal de Regulação de Serviços Públicos Delegados de Cachoeiro de Itapemirim
CNPJ Contratante	03.311.730/0001-00
Contratado	DATACI – Companhia de Tecnologia da Informação de Cachoeiro de Itapemirim
CNPJ Contratado	31.720.485/0001-11
Objeto	Supressão de 10% (dez por cento) do valor mensal do Contrato e a retificação do prazo de vigência do contrato
Do valor	Com o presente aditivo o valor mensal do contrato após a supressão é de R$ 2.700,00 (dois mil e setecentos reais), perfazendo o valor anual de R$ 32.400,00 (trinta e dois mil e quatrocentos reais) e valor global de 133.200,00 (cento e trinta e três mil e duzentos reais)
Do prazo de vigência	Retificação do prazo de vigência do contrato publicado em 23/09/2014
Data de Assinatura	23/09/2015
Vigência do Contrato	48 (quarenta e oito meses) a contar do dia subsequente a publicação do resumo do Diário Oficial do Município
Signatários	Fernando Santos Moura (Diretor Presidente da AGERSA), Edmar Lyrio Temporim (Diretor Presidente da DATACI) e Carla da Costa Araujo (Diretora de Tecnologia de Gestão DATACI)
Ano Processo	2014
Nº Processo	1188458 (Protocolo AGERSA n°. 15562/2014)
Fundamento Legal	Lei 8.666/1993, artigos 24, VIII / XVI, 57, IV e 65 §1°

FERNANDO SANTOS MOURA
Diretor Presidente

ATOS DO PODER LEGISLATIVO MUNICIPAL

DECRETO LEGISLATIVO Nº 2434/2015.

RATIFICA AS INSTRUÇÕES NORMATIVAS STI Nº 01 e 02/2015 – VERSÃO 01.

O PRESIDENTE DA CÂMARA MUNICIPAL DE CACHOEIRO DE ITAPEMIRIM, ESTADO DO ESPÍRITO SANTO, NO USO DE SUAS ATRIBUIÇÕES LEGAIS,

RESOLVE:

Art. 1º – Ratifica as Instruções Normativas STI nº 01 e 02/2015 – versão 01, conforme anexos.

Art. 2º - Este Decreto entrará em vigor na data de sua publicação.

Cachoeiro de Itapemirim-ES, 29 de setembro de 2015.

JULIO CESAR FERRARE CECOTTI
Presidente

INSTRUÇÃO NORMATIVA STI nº. 01/2015

Versão: 01
Aprovada em: 29 de setembro de 2015
Ato de Aprovação: Decreto Legislativo nº 2434/2015
Unidade Responsável: Sistema de Tecnologia da Informação - STI

I – FINALIDADE
A presente Instrução Normativa tem por objetivo disciplinar os procedimentos administrativos do STI quanto a segurança física e lógica dos equipamentos, sistemas, dados e informações, contra acessos não autorizados, acidentes naturais e danos intencionais, políticas de Segurança da Informação, procedimentos de utilização de Internet e procedimentos de utilização do Correio Eletrônico Corporativo.

II – ABRANGÊNCIA
A presente Instrução Normativa todas as unidades da estrutura organizacional da CMCI, sendo todos usuários dos serviços de informática.

III – CONCEITOS
1 – Tecnologia da Informação - Entende-se como Tecnologia da Informação o conjunto de recursos tecnológicos e computacionais para geração e uso da informação. Para os fins da presente Instrução Normativa, o termo designa o conjunto de recursos não humanos dedicados ao armazenamento, processamento e comunicação da informação, bem como, o modo como esses recursos estão organizados em um sistema capaz de executar um conjunto de tarefas.
2 – Recursos Computacionais - Para os efeitos dessa Instrução, Recursos Computacionais se referem a todos os equipamentos, as instalações ou banco de dados direta ou indiretamente administrados, mantidos ou operados pela CMCI, compreendendo: Computadores e Notebooks de quaisquer espécies, incluídos seus equipamentos acessórios; Impressoras, Scanners e equipamentos multifuncionais; Redes de computadores e de transmissão de dados; Banco de Dados ou documentos residentes em disco, fita magnética ou outros meios; Leitoras de códigos de barras; Racks, Patch Panel, Switches, Access Points e Routers Wireless entre

outros equipamentos de rede; Software, sistemas e programas adquiridos ou desenvolvidos pela Administração.

3 – Usuário - É todo agente público da CMCI ou prestador de serviço que necessite de acesso à rede corporativa ou utilize algum recurso computacional da instituição.

4 – Unidade Usuária - Corresponde a qualquer unidade administrativa, que utilize os recursos computacionais integrantes da estrutura da CMCI.

5 – Segurança Física - A Segurança Física tem como objetivo proteger recursos computacionais contra usuários não autorizados, prevenindo o acesso a esses recursos. A Segurança Física deve se basear em perímetros predefinidos nas imediações dos recursos computacionais, podendo ser explícita como uma sala-cofre, ou implícita, como áreas de acesso restrito. A Segurança Física pode ser compreendida em dois (02) aspectos:

a) Segurança de Acesso: Trata das medidas de proteção contra o acesso físico não autorizado;

b) Segurança Ambiental: Trata-se da prevenção de danos por causas naturais;

6 – Segurança Lógica - A Segurança Lógica é um processo pelo qual um sujeito ativo deseja acessar um objeto passivo. O sujeito é um usuário ou um processo da rede e o objeto pode ser um arquivo ou outro recurso de rede (Estação de Trabalho, Impressora, etc.). a Segurança Lógica compreende um conjunto de medidas e procedimentos adotados pela instituição ou intrínsecos aos sistemas utilizados. O objetivo é proteger os dados, programas e sistemas contra tentativas de acessos não autorizados, feitas por usuários ou outros programas. Na Segurança Lógica, pretende-se proteger recursos e informações referentes a: Aplicativos (Programas Fonte e Objeto); Arquivos de Dados; Utilitários e Sistema Operacional; Arquivos de Senha e Arquivos de Log.

7 – Sistema - Para os efeitos desta Instrução Normativa, a palavra Sistema terá o seguinte conceito: "Um conjunto organizado de componentes para coletar, transmitir, armazenar e processar dados de modo a fornecer informação para a ação". (ZWASS, 1998).

8 – Dados e Informações - Segundo LE COADIC (2004), dados são uma representação composta de informação codificada de uma forma a permitir coloca-las sob processamento eletrônico. Já para TURBAN (2003), os dados são nada mais que a matéria prima da informação. Os dados são descrições de coisas, eventos e atividades os quais sozinhos não conseguem se unir e representar algum significado. Já SOUZA (2006) diz que os dados são uma sequencia de símbolos codificados de tal forma a permitir sua manipulação pelo computador. De acordo com as três (03) opiniões citadas acima, resume-se dados como sendo a matéria prima da informação a qual deve ser representada de forma a permitir a sua manipulação pelo computador.

De acordo com ZEMAN (1970), o temo informação se resume na ideia de dar forma e representar uma ideia. Para ele, informações são dados contextualizados para algum propósito. Já para SHANNON, informação é algo recebido por um receptor de um transmissor em um processo de comunicação. Igualmente DAVENPORT e PRUSAK concordam com SHANNON no que diz respeito a informação ser resultado da comunicação entre transmissor e um receptor. Desta forma, resume-se informação como sendo algo que dá forma a uma determinada ideia e surge como resultado da comunicação entre um receptor e um transmissor.

9 – Processamento de Dados - Conceitua-se como Processamento de Dados uma série de atividades ordenadamente realizadas, que resultará em uma espécie de arranjo de informações, pois no inicio da atividade é feita a coleta de informações, ou dados, que passam por uma organização onde no final será passada para o usuário o dado pertinente a sua busca.

IV – BASE LEGAL E REGULAMENTAR

I – Constituição Federal de 1988;
II – Lei Orgânica do Município de Cachoeiro de Itapemirim/ES;
III – Lei Federal nº 9.609/1998;
IV – ISO 27001;
V – Demais legislações pertinentes.

V – RESPONSABILIDADES

1. Da Unidade Responsável pela Instrução Normativa:
- Promover a divulgação desta Instrução Normativa, mantendo-a atualizada;
- Orientar as áreas executoras e supervisionar sua aplicação;
- Promover discussões técnicas com as unidades executoras e com a unidade responsável pela coordenação do controle interno, para definir as rotinas de trabalho e os respectivos procedimentos de controle que devem ser objeto de alteração, atualização ou expansão;
- Manter atualizada, orientar as áreas executoras e supervisionar a aplicação desta Instrução Normativa.

2. Das Unidades Executoras:
- Atender às solicitações da unidade responsável pela Instrução Normativa, quanto ao fornecimento de informações e à participação no processo de atualização;
- Alertar a unidade responsável pela Instrução Normativa sobre as alterações que se fizerem necessárias nas rotinas de trabalho, objetivando a sua otimização, tendo em vista,
principalmente, o aprimoramento dos procedimentos de controle e o aumento da eficiência operacional;
- Manter a Instrução Normativa à disposição de todos os servidores da unidade, velando pelo fiel cumprimento da mesma;
- Cumprir fielmente as determinações da Instrução Normativa, em especial quanto aos procedimentos de controle e quanto à padronização dos procedimentos na geração de documentos, dados e informações.

3. Da Unidade Responsável pela Coordenação do Controle Interno:
- Prestar apoio técnico por ocasião das atualizações desta Instrução Normativa, em especial no que tange à identificação e avaliação dos pontos de controle e respectivos procedimentos de controle;
- Através da atividade de auditoria interna, avaliar a eficácia dos procedimentos de controle inerentes ao SRH, propondo alterações na Instrução Normativa para aprimoramento dos controles.

VI – PROCEDIMENTOS

A – Obrigações e Permissões dos Usuários:

1.Para utilizar os computadores, internet, rede corporativa da CMCI, softwares, aplicativos e pastas em geral, o usuário deverá solicitar com antecedência, à chefia imediata, a abertura de uma conta de acesso (login) e senha;

2. O formulário "Controle de acesso aos sistemas", Anexo I, deve ser assinado, na qualidade de solicitante, pelo superior imediato do servidor ou titular responsável pelo setor à quem está concedendo o acesso;

3. Nos casos de demissão, exoneração, aposentadoria ou qualquer outro que implique o desligamento do usuário do Poder legislativo, o chefe imediato do usuário deverá comunicar imediatamente o fato ao DTI, por meio do formulário "Controle de Acesso aos Sistemas", Anexo I, assinalando no quadro a opção "exclusão";

4. Nos casos de transferência de local de trabalho, o chefe imediato do usuário deverá comunicar imediatamente o fato à DTI, por meio do formulário constante no Anexo I, assinalando a opção "Alteração";

5. Toda conta de acesso é atribuída à uma única pessoa e será de responsabilidade e de uso exclusivo de seu titular, não podendo esse permitir ou colaborar com o acesso aos recursos computacionais

por parte de pessoas não autorizadas e nem compartilhar com outros usuários;
6. O descumprimento do Termo de Responsabilidade, Anexo II, caracteriza infração funcional, podendo ocasionar a responsabilização civil, administrativa e penal do infrator;
7. O perfil de acesso dos usuários aos aplicativos e sistemas será o necessário para o desempenho de suas atividades;
8. O usuário será responsável pela segurança de sua conta de acesso e senha, pelas informações armazenadas nos equipamentos dos quais faz uso e por qualquer atividade neles desenvolvida;
9. Uma senha segura deverá conter no mínimo seis (06) caracteres alfanuméricos (letras e números)

10. As contas inativas por mais de sessenta (60) dias serão desabilitadas. O usuário que pretenda preservar seus dados deverá comunicar seu afastamento com antecedência;
11 . As contas de acesso dos prestadores de serviços e servidores temporários deverão ser automaticamente bloqueadas na data de término de contrato;

B – Estações de Trabalho e Componentes:
1 – O usuário deverá executar somente tarefas e aplicações que estejam dentro do escopo de trabalho de seu setor, utilizando os programas e equipamentos com zelo e responsabilidade;
2 – Caberá aos usuários comunicar imediatamente à Administração quaisquer problemas que venham ocorrer, bem como relatar qualquer suspeita de uso inadequado dos recursos computacionais;
3 – Não será permitido aos usuários alterar, configurar ou remanejar estações de trabalho e periféricos de seus locais de instalação sem o conhecimento do DTI;
4 - Não deverão ser conectados Notebooks, Laptops, Tablets ou outros equipamentos aos computadores da CMCI sem o conhecimento da DTI;
5 – Apenas dispositivos como Laptops, Notebooks, Tablets entre outros de propriedade da CMCI ou que se enquadrem aos padrões de segurança exigidos pela Câmara, poderão ser conectados na rede de computadores;
6 – É vedada a abertura de computadores para qualquer tipo de reparo. Caso o mesmo seja necessário, o mesmo deverá ser reportado e realizado única e exclusivamente pelo DTI;
7 – Algumas configurações de desktop (papel de parede, opções de menu, configurações, etc.) poderão ser controladas e padronizadas pelo DTI;
8 – Os usuários, a menos que tenham uma autorização específica para este fim, não poderão tentar, permitir ou causar qualquer alteração ou destruição de ambientes operacionais, dados ou equipamentos de processamento ou comunicações instalados na CMCI;
9 – Com exceção das estações de trabalho, impressoras e estabilizadores, os usuários não poderão ligar ou desligar fisicamente ou eletricamente equipamentos da CMCI sem autorização prévia do DTI, especialmente os equipamentos de rede como Switches e Servidores;
10 – Não será permitida a utilização dos recursos computacionais para benefício próprio ou de terceiros, direto ou indireto, sujeitando-se o infrator à imediata suspensão der sua chave de acesso, sem prejuízo da aplicação das demais penalidades cabíveis;
11 – Não será permitido carregar e executar qualquer tipo de jogos, bem como áudio e vídeos e armazenar tais arquivos no servidor ou na estação de trabalho que não sejam compatíveis com as atividades desenvolvidas no setor;
12 – Os usuários deverão manter os equipamentos nas suas perfeitas condições de uso na forma como lhes foram entregues, evitando a colagem de adesivos ou outros enfeites particulares e realizando a devida limpeza física superficial dos equipamentos;
13 – Não deverão colocar objetos sobre os equipamentos de forma a prejudicar seu sistema de ventilação, assim como manipular líquidos, alimentos ou substâncias que possam ocasionar danos quando os estiver operando;
14 – O usuário deverá encerrar a sua sessão (desligar ou fazer logoff) na estação de trabalho ao término de suas atividades, devendo, no final do expediente, a estação de trabalho permanecer desligada, bem como sua impressora e nobreak (se aplicáveis);

C – Ambiente de Rede:
1 – O DTI disponibilizará os pontos de rede necessários ao desenvolvimento das atividades dentro de seu(s) prédio(s), devendo para qualquer alteração ou criação de um ponto novo o ser comunicado em tempo hábil;

2 – É proibido o uso de meios ilícitos de acesso aos computadores, sistemas e arquivos do ambiente de rede computacional da CMCI;
3 – É proibido o acesso remoto aos computadores da rede da CMCI sem o conhecimento e subsequente autorização do DTI;
4 – Não será permitido o uso de quaisquer materiais ou informações, incluindo arquivos, textos, planilhas ou imagens disponíveis na rede corporativa da CMCI, que não respeitem os direitos autorais, marcas registradas, patentes, sigilos comerciais ou outros direitos de propriedade intelectual de terceiros;
5 – Não será permitida a alteração das configurações de rede e do sistema das máquinas, bem como modificações que possam trazer algum problema futuro;
6 – É proibido tentar burlar a utilização dos recursos computacionais da CMCI, com o objetivo de obter proveito pessoal ou violar sistemas de segurança estabelecidos;
7 – Os usuários não poderão instalar ou fazer “upgrade” de qualquer espécie de programas ou aplicativos na estação de trabalho sem aprovação do DTI;
8 – Não será permitido o uso, para fins particulares ou de recreação de serviços que sobrecarreguem a rede computacional, tais como rádios on-line, páginas de animação, visualização de apresentações, vídeos, jogos, conteúdo pornográfico, entre outros;
9 – Com relação aos sistemas de ensino baseados na web (Internet), só será permitido o acesso àqueles que fazem jus ao seu uso no âmbito dessa Câmara Municipal por se tratarem de aperfeiçoamento e apoio para as atividades laborais do usuário, excluindo-se toda e qualquer consulta que resulte em benefício pessoal e unitário tão somente para o usuário;

D – Correio Eletrônico Institucional (e-mail):
1 – O acesso ao sistema de correio eletrônico será disponibilizado aos usuários com necessidade manifesta de usá-lo como ferramenta de apoio às atividades profissionais, a ordem e uma (01) caixa de e-mail por setor, podendo ocasionalmente ser utilizado para mensagens pessoais curtas e pouco frequentes;
2 – Não será permitido participar, criar ou distribuir voluntariamente mensagens indesejáveis como circulares, manifestos políticos, correntes de cartas ou similares que possam prejudicar o trabalho de terceiros, causar tráfego excessivo na rede ou sobrecarregar os sistemas computacionais desnecessariamente;
3 – Ficará proibido utilizar os serviços para envio de SPAM, ou seja, o envio em massa de e-mails para usuários que não os solicitarem de forma explícita e com os quais o remetente não mantenha qualquer vínculo de relacionamento profissional e cuja quantidade comprometa o bom funcionamento dos servidores de e-mail;
4 – Não será permitido o uso de endereços de e-mail para troca de informações ligadas à práticas que infrinjam qualquer lei nacional ou internacional;
5 – O usuário não deverá abrir e-mails com arquivos anexados

quando não conhecer o remetente, sob o risco de infectar com vírus o seu equipamento;

E – Internet:
1 – O uso de internet deverá ser controlado e restrito às atividades profissionais, no sentido de manter os mais altos níveis de qualificação e segurança em prol da atualização da informação;
2 – Será inaceitável utilizar-se dos serviços internos de internet da CMCI desviando-se de sua finalidade, com o intuito de cometer fraudes;
3 – É proibido visualizar, criar, postar, carregar ou encaminhar quaisquer arquivos ou mensagens de conteúdos abusivos, obscenos, insultuosos, sexualmente tendenciosos, pornográficos, ofensivos, difamatórios, agressivos, ameaçadores, vulgares, racistas, de apologia ao uso de drogas, de incentivo à violência ou outro material que possa violar qualquer lei aplicável;
4 – Não será permitido acessar salas de bate-papo (chat rooms), jogos, apostas e assemelhados;
5 – Não será permitido desfrutar de quaisquer ferramentas Peer-to-peer para baixar músicas, vídeos, ou jogos, tais como *E-mule, Kazaa, IMesh, Ares, AudioGalaxy, WinMX, Gnutella, LimeWire, uTorrent, BitTorrent,* aceleradores de download e outros aplicativos afins;
6 – Não será permitido fazer download de arquivos cujo conteúdo não tenha relação com as atividades realizadas pela CMCI;
7 - Ficará proibida a utilização de ferramentas que burlem a segurança e regras de proxy/firewall com o intuito de usufruir de serviços que não lhes dão concebidos, como por exemplo, Ultrasurf;
8 – Ficará ao cargo do chefe imediato do departamento a solicitação do bloqueio de outros sites que não estejam relacionados neste documento ou previamente bloqueados de acordo com as regras de governança de T.I. no setor público estabelecidas pela União. Esse bloqueio afetará somente o departamento solicitante;
9 – O sistema de filtro de acessos gerará relatórios periódicos indicando os usuários que eventualmente navegam e/ou acessam recursos da internet indevidamente. Esses relatórios são gerados por usuário e poderá ser solicitado pela chefia imediata;
10 – Não será permitida a utilização de software não homologado pelo DTI para ser o cliente de navegação;
11 – Não será permitida a manutenção não autorizada de páginas pessoais ou de serviços particulares envolvendo comercialização pela internet utilizando os recursos computacionais da CMCI;

F – Armazenamento de Documentos e Informações:
1 – O usuário deverá manter sigilo sobre os documentos e informações considerados estratégicos, confidenciais ou de interesse particular da CMCI;
2 – Todos os documentos e informações dos setores administrativos da CMCI deverão ser armazenados nos diretórios em pastas devidamente identificadas por departamento;
3 – O usuário deverá informar ao seu superior imediato quando informações ou aplicações consideradas estratégicas ou confidenciais forem encontradas sem o tratamento de segurança correto;
4 – Os documentos e informações geradas pelos usuários referentes às rotinas de trabalho, no que diz respeito à alterações, gravações e leituras, são de inteira responsabilidade dos usuários do arquivo;
5 – Os arquivos do diretório raiz (C:\) poderão ser removidos sempre que não condizerem com a estrutura do sistema operacional ou de software, relevantes para a Administração, independentemente do seu conteúdo;

G – Advertências e Penalidades:
1 – Os usuários deverão estar cientes das regras e normas de uso dos recursos computacionais evitando deste modo os procedimentos que prejudiquem ou impedem outras pessoas de terem acesso a esses recursos ou de usá-los de acordo com o que é determinado;
2 – Todo servidor que tiver conhecimento de ato ilícito praticado no uso dos recursos computacionais, assim como qualquer comportamento considerado inaceitável ou suspeito de violação dessas normas, deverá comunicar o fato imediatamente a seu superior imediato e ao DTI;
3 – A Administração se resguardará do direito de monitorar e interferir no tráfego de rede da CMCI, sempre que julgar necessário e sem aviso prévio, com o propósito de verificar o cumprimento dos padrões de segurança, além de fiscalizar e auditar todos os recursos computacionais;

H – Responsabilidades do Departamento de Tecnologia da Informação:
1 – Cabe ao DTI definir as pessoas que poderão ter acesso físico e lógico ao servidor de rede e tomar as medidas necessárias para inibir o acesso aos usuários cujas concessões lhe foram total ou parcialmente alteradas ou canceladas;
2 – O DTI deverá avaliar e definir a ordem de relevância de cada aplicativo, segundo o grau de dependência da organização de cada um deles, atentando para as medidas de segurança para os mais importantes;
3 – Quando se fizer necessário, o DTI deverá fazer os encaminhamentos para a aplicação de penalidades, nos casos constatados de violações aos ambientes de processamento de dados e demais inobservâncias à presente Instrução Normativa;
4 – Com respeito à segurança lógica, deverá ser feita a manutenção de cópias (Back-up) de segurança dos sistemas em local seguro e protegido contra sinistros, com execução de testes periódicos objetivando aferir, se em caso de emergência, os arquivos disponíveis possibilitariam a retomada integral do processamento de dados;
5 – Orientar as áreas usuárias na definição do Back-up dos arquivos operacionais e de segurança, na proteção contra o acesso não autorizado aos aplicativos, para consulta e/ou atualização, em nível de diretórios, sistema, rotina/programa, arquivo ou dado;
6 – Definir em conjunto com as unidades geradoras de documentos e arquivos, quais unidades que poderão ter acesso aos mesmos via rede, por tipo de documento e informação e manutenção das tabelas para liberação de acesso;
7 – Efetuar a manutenção do funcionamento, segurança e confiabilidade da rede interna, com análise regular dos registros de sua utilização, com investigação sobre as tentativas bloqueadas de acesso;
8 – No tocante á segurança física, o DTI deverá definir as medidas para a proteção física do acervo de processamento de dados da CMCI, a serem observadas durante e fora do expediente normal, por todas as unidades usuárias;

I – Responsabilidades das Unidades Usuárias dos Recursos Computacionais:
1 – Supervisionar e gerenciar a execução das tarefas de T. I., incluindo a definição de pessoas que poderão ter acesso (físico e lógico) aos equipamentos e respectivos softwares instalados na unidade;
2 – Definir os níveis de acesso (consulta/atualização) aos, sistemas, rotinas/programas, arquivos e dados, para todos os aplicativos de responsabilidade de sua área;
3 – Conceder autorização do acesso a dados e informações, via rede, pelos diversos usuários, aos sistemas e/ou aplicativos cuja operação é de sua competência, mantendo o registro das autorizações concedidas;
4 – Fazer a utilização do produto de antivírus de acordo com as

instruções recebidas do DTI;
5 – Comunicar ao DTI todas as situações que ensejarem manutenção da rede e dos equipamentos de processamento de dados sob sua responsabilidade;

VII – CONSIDERAÇÕES FINAIS
1 – Os termos contidos nessa Instrução Normativa não eximem a observância das demais normas competentes, que deverão ser respeitadas.
2 – Os esclarecimentos adicionais a respeito deste documento poderão ser obtidos junto à UCCI da CMCI que, por sua vez, através de procedimentos de checagem (visitas de rotinas) ou auditoria interna, aferirá a fiel observância de seus dispositivos por parte das diversas unidades da Estrutura Organizacional bem como também ao DTI.

3 – A inobservância das normas estabelecidas nesta Instrução Normativa pelos agentes públicos acarretará instauração de procedimento administrativo para apurar responsabilidade conforme rege o Estatuto dos Servidores Públicos Municipais e demais sansões previstas na legislação pertinente à matéria em vigor.

Esta Instrução Normativa entra em vigor a partir da sua aprovação.

Cachoeiro de Itapemirim/E.S, 15 de Setembro de 2015.

PABLO LORDES DIAS
Controlador Interno Geral

WAGNER BAPTISTA RUBIM
Controlador de Recursos

RONALDO CRUZ GARCIA JUNIOR
depto. Responsável - Supervisor de Informática

INSTRUÇÃO NORMATIVA STI Nº. 001/2015

Anexo I

CÂMARA MUNICIPAL DE CACHOEIRO DE ITAPEMIRIM
ESTADO DO ESPÍRITO SANTO

Departamento de Tecnologia da Informação

Controle de Acesso aos Sistemas

□ CADASTRO □ ALTERAÇÃO □ EXCLUSÃO

NOME: _____
LOGIN: _____
DATA DE NASCIMENTO: _____/_____/_____
CELULAR: _____ SETOR: _____
E-MAIL: _____
CARGO: _____

SOLICITO A HABILITAÇÃO DO USUÁRIO IDENTIFICADO NOS SEGUINTES SISTEMAS:
□ Acesso à rede □ Almoxarifado □ Contabilidade □ Protocolo □ Patrimônio □ RH □ Financeiro

SOFTWARES QUE POSSUI CONHECIMENTO:
□ Windows 8 □ Linux □ Word □ Excel □ PowerPoint □ LibreOffice □ CorelDraw!

DATA: ___/___/_____

_____
Assinatura / Carimbo

INSTRUÇÃO NORMATIVA STI Nº. 001/2015

Anexo II

CÂMARA MUNICIPAL DE CACHOEIRO DE ITAPEMIRIM
ESTADO DO ESPÍRITO SANTO

Departamento de Tecnologia da Informação

Termo de Responsabilidade – Uso de sistemas

Eu, _____, declaro haver solicitado acesso ao(s) sistema(s) _____, comprometendo-me a utilizá-lo(s) conforme a IN STI 01/2015.

Cachoeiro de Itapemirim-ES, aos _____ de ____ de 20_____.

Usuário_____

Departamento de T. I. _____

INSTRUÇÃO NORMATIVA STI Nº. 002/2015

Versão: 01
Aprovada em: 29 de setembro de 2015
Ato de Aprovação: Decreto Legislativo nº 2434/2015
Unidade Responsável: Sistema de Tecnologia da Informação - STI

I – FINALIDADE
A presente Instrução Normativa tem por objetivo disciplinar os procedimentos administrativos do STI quanto a aquisição, locação e utilização de *software, hardware, suprimentos e serviços de T. I.*

II – ABRANGÊNCIA
A presente Instrução Normativa todas as unidades da estrutura organizacional da CMCI, sendo todos usuários dos serviços de informática.

III – CONCEITOS
1 – Hardware - Para o DTI, o termo "*hardware*" é usado para fazer referência a detalhes específicos de uma dada máquina, incluindo-se o seu projeto lógico pormenorizado, bem como a tecnologia de embalagem da máquina (Hennessy, John L.; Patterson, David A, 2003). O termo "*hardware*" não se refere apenas aos computadores pessoais, mas também aos produtos que necessitam de processamento computacional, tais como Impressoras, Nobreak, Telefones, Switches, entre outros.
2 – Software - é uma sequência de instruções escritas para serem interpretadas por um computador com o objetivo de executar tarefas específicas. Em um computador, o *software* é classificado como a parte lógica cuja função é fornecer instruções para o *hardware*.
2.1 – *Software* Livre ou não proprietários – são aqueles que estão sobre uma licença livre (p. ex. GNU) e que seu

uso, modificação e distribuição são permitidos à todos. *Software* livre não é sinônimo de gratuidade.

2.2 – *Software* Proprietário – Os *Softwares* Pagos ou proprietários são aqueles que tem um dono e o seu uso se dá mediante a uma licença comercial e na maioria das vezes paga. Os *softwares* pagos não são comercialmente diferentes de qualquer outro produto, apenas observando que mesmo pagando por um *software* você estará recebendo apenas a licença ou direito de uso e não comprando o *software* propriamente dito.

3 – Serviços de T. I. - Conjunto de componentes relacionados que são utilizados no fornecimento de suporte a uma ou mais unidades da CMCI. Pode ser visto também como a combinação de hardware, software, processos e pessoas, com o objetivo de gerar um serviço para satisfazer uma ou mais necessidades de um cliente.

IV – BASE LEGAL E REGULAMENTAR

I – Constituição Federal de 1988;
II – Lei Orgânica do Município de Cachoeiro de Itapemirim/ES;
III – Lei Federal nº 9.609/1998;
IV – ISO 27001;
V – Lei Federal nº 8.666/93;
VI – Demais legislações pertinentes.

V – RESPONSABILIDADES

1. Da Unidade Responsável pela Instrução Normativa:
- Promover a divulgação desta Instrução Normativa, mantendo-a atualizada;
- Orientar as áreas executoras e supervisionar sua aplicação;
- Promover discussões técnicas com as unidades executoras e com a unidade responsável pela coordenação do controle interno, para definir as rotinas de trabalho e os respectivos procedimentos de controle que devem ser objeto de alteração, atualização ou expansão;
- Manter atualizada, orientar as áreas executoras e supervisionar a aplicação desta Instrução Normativa.

2. Das Unidades Executoras:
- Atender às solicitações da unidade responsável pela Instrução Normativa, quanto ao fornecimento de informações e à participação no processo de atualização;
- Alertar a unidade responsável pela Instrução Normativa sobre as alterações que se fizerem necessárias nas rotinas de trabalho, objetivando a sua otimização, tendo em vista,
principalmente, o aprimoramento dos procedimentos de controle e o aumento da eficiência operacional;
- Manter a Instrução Normativa à disposição de todos os servidores da unidade, velando pelo fiel cumprimento da mesma;
- Cumprir fielmente as determinações da Instrução Normativa, em especial quanto aos procedimentos de controle e quanto à padronização dos procedimentos na geração de documentos, dados e informações.

3. Da Unidade Responsável pela Coordenação do Controle Interno:
- Prestar apoio técnico por ocasião das atualizações desta Instrução Normativa, em especial no que tange à identificação e avaliação dos pontos de controle e respectivos procedimentos de controle;
- Através da atividade de auditoria interna, avaliar a eficácia dos procedimentos de controle inerentes ao SRH, propondo alterações na Instrução Normativa para aprimoramento dos controles.

VI – PROCEDIMENTOS

A – SOFTWARE

1. Todo *software* utilizado na CMCI deverá ser homologado pelo DTI, anteriormente a sua contratação. Os software já adquiridos anteriormente a esta norma, pela modalidade de locação, deverão passar pelo crivo e necessária homologação do DTI quando da sua posterior renovação;
2. Os usuários não poderão instalar ou fazer "*upgrade*" de qualquer espécie de programas ou aplicativos nas estações de trabalho sem aprovação do DTI;
3. Software proprietário (Licença Paga) só poderá ser instalado e utilizado após aquisição das respectivas licenças ou mediante a locação junto ao proprietário;
4. Não será permitida a utilização de softwares "piratas";
5. Os termos e condições sob os quais o Licenciante prestará serviços ao Licenciado em relação a produtos de *software* licenciado devem estar descritos no próprio contrato, assinados pelas partes e mediante a contraprestação do pagamento pelos mesmos;
6. Quaisquer instalações, após devida aprovação, deverá ser comunicada ao DTI, que deverá ser analisada com intuito de não causar conflito com banco de dados e outros *software*;
7. Por medidas de segurança e compatibilidade entre os aplicativos, o DTI poderá negar a utilização de alguns *softwares,* baseado em laudo técnico emitido pelo DTI e seu subsequente aceite pelo departamento usuário do respectivo software;

B – HARDWARE:

1 – Toda a solicitação de compra ou locação de equipamentos de informática deverá ser analisada pelo DTI, com o intuito de manter as configurações mínimas exigidas nos modelos desenvolvidos por essa divisão;
2 – O DTI será responsável por verificar a compatibilidade dos equipamentos de informática com a estrutura de rede da CMCI e a observância de um processo mínimo e progressivo de padronização de recursos no âmbito da Administração;
3 – Toda aquisição de bens do tipo equipamentos de informática deverão ser adquiridos com garantia e prestação da correspondente assistência técnica pelo prazo mínimo de um (01) ano contado a partir da sua efetiva entrega;
4 – Deverá ser exigido no edital a disponibilidade de prestação dos serviços de assistência técnica em território estadual, diretamente ou através de estabelecimento, filial ou empresas consorciadas ou subcontratadas;
5 – Equipamentos de informática a serem adquiridos deverão conter a inclusão do sistema operacional mínimo para o seu funcionamento (Windows);
6 – Será exigido no edital, que o prazo de entrega máximo do lote integral ou do primeiro lote de equipamentos deverá ser em até trinta (30) dias contados da assinatura do contrato ou do protocolo da respectiva ordem de fornecimento;
7 – Não se classifica como equipamento de informática: o mobiliário e instalações utilizadas para as disposições dos computadores e equipamentos de informática, o material de consumo e suprimento básico para o funcionamento dos equipamentos de informática (papel para impressão, formulários, cartuchos ou fitas para impressoras, CD, DVD, entre outros suprimentos);

VII – CONSIDERAÇÕES FINAIS

1 – Os termos contidos nessa Instrução Normativa não eximem a observância das demais normas competentes, que deverão ser respeitadas.
2 – Os esclarecimentos adicionais a respeito deste documento poderão ser obtidos junto à UCCI da CMCI que, por sua vez, através de procedimentos de checagem (visitas de rotinas) ou auditoria interna, aferirá a fiel observância de seus dispositivos por parte das diversas unidades da Estrutura Organizacional, bem como pelo DTI.
3 – A inobservância das normas estabelecidas nesta Instrução Normativa pelos agentes públicos acarretará instauração de

procedimento administrativo para apurar responsabilidade conforme rege o Estatuto dos Servidores Públicos Municipais e demais sansões previstas na legislação pertinente à matéria em vigor.

Esta Instrução Normativa entra em vigor a partir da sua aprovação.

Cachoeiro de Itapemirim/ES, 15 de Setembro de 2015.

PABLO LORDES DIAS
Controlador Interno Geral

WAGNER BAPTISTA RUBIM
Controlador de Recursos

RONALDO CRUZ GARCIA JUNIOR
depto. Responsável - Supervisor de Informática

DECRETO LEGISLATIVO Nº 2435/2015.

RATIFICA A INSTRUÇÃO NORMATIVA SPC Nº 01/2015 – VERSÃO 01.

O PRESIDENTE DA CÂMARA MUNICIPAL DE CACHOEIRO DE ITAPEMIRIM, ESTADO DO ESPÍRITO SANTO, NO USO DE SUAS ATRIBUIÇÕES LEGAIS,

RESOLVE:

Art. 1º – Ratifica a Instrução Normativa SPC nº 01/2015 – versão 01, conforme anexo.

Art. 2º - Este Decreto entrará em vigor na data de sua publicação.

Cachoeiro de Itapemirim-ES, 29 de setembro de 2015.

JULIO CESAR FERRARE CECOTTI
Presidente

INSTRUÇÃO NORMATIVA SPC nº. 01/2015
Versão: 01
Aprovada em: 29 de setembro de 2015
Ato de Aprovação: Decreto Legislativo nº 2435/2015
Unidade Responsável: Sistema de Publicidade e Comunicação – SPC

I - FINALIDADE
Normatizar os procedimentos relativos à gestão das ações de publicidade da Câmara Municipal.

II - ABRANGÊNCIA
Abrange todas as unidades da estrutura organizacional da CMCI que dão origem aos atos relacionados à gestão de publicidade.

III - CONCEITOS
1 - PUBLICIDADE INSTITUCIONAL - a que se destina a divulgar atos, ações, programas, obras, serviços, campanhas, metas e resultados da Câmara Municipal, com o objetivo de atender ao princípio da publicidade, de valorizar e fortalecer o poder público e de estimular a participação da sociedade no debate, no controle e na formulação de políticas públicas.
2- PUBLICIDADE DE UTILIDADE PÚBLICA - a que se destina a divulgar direitos e serviços colocados à disposição dos cidadãos, oriundos da ação da Câmara Municipal, com o objetivo de informar, educar, orientar, mobilizar, prevenir ou alertar a população para adotar comportamentos que lhe tragam benefícios individuais ou coletivos e que melhorem a sua qualidade de vida;

3 - PUBLICIDADE LEGAL - a que se destina a dar conhecimento de editais, balanços, atas, decisões, realização de audiências públicas e outras reuniões, avisos e de outras informações da Câmara Municipal, com o objetivo de atender a prescrições legais.

IV - BASE LEGAL E REGULAMENTAR
I – Constituição Federal de 1988
II - Lei Nº 101/2000 - Lei de Responsabilidade Fiscal (LFR)
III - Lei Complementar Nº 131/2009 - Lei da Transparência
IV - Lei Nº 12.232/2010 - Dispõe sobre as normas gerais para licitação e contratação pela Administração Pública de serviços de publicidade prestados por meio de agências de propaganda.
V - Decreto nº 7.185 - regulamentação do art. 48 da LRF
VI - Lei Nº 12.527/2011 - Lei de Acesso à Informação
VII - Decreto Nº 7.724/2012 – regulamentação da Lei de Acesso à Informação
VIII - Lei Orgânica do Município de Cachoeiro de Itapemirim/ES
XIX - Demais legislações pertinentes

V - RESPONSABILIDADES
1. Da Unidade Responsável pela Instrução Normativa:
- Promover a divulgação desta Instrução Normativa, mantendo-a atualizada;
- Orientar as áreas executoras e supervisionar sua aplicação;
- Promover discussões técnicas com as unidades executoras e com a unidade responsável pela coordenação do controle interno, para definir as rotinas de trabalho e os respectivos procedimentos de controle que devem ser objeto de alteração, atualização ou expansão;
-

- Manter atualizada, orientar as áreas executoras e supervisionar a aplicação desta Instrução Normativa.

2. Das Unidades Executoras:
- Atender às solicitações da unidade responsável pela Instrução Normativa, quanto ao
fornecimento de informações e à participação no processo de atualização;
- Alertar a unidade responsável pela Instrução Normativa sobre as alterações que se fizerem necessárias nas rotinas de trabalho, objetivando a sua otimização, tendo em vista,
principalmente, o aprimoramento dos procedimentos de controle e o aumento da eficiência operacional;
- Manter a Instrução Normativa à disposição de todos os servidores da unidade, velando pelo fiel cumprimento da mesma;
- Cumprir fielmente as determinações da Instrução Normativa, em especial quanto aos
procedimentos de controle e quanto à padronização dos procedimentos na geração de
documentos, dados e informações.

3. Da Unidade Responsável pela Coordenação do Controle Interno:
- Prestar apoio técnico por ocasião das atualizações desta Instrução Normativa, em especial no que tange à identificação e avaliação dos pontos de controle e respectivos procedimentos de controle;
- Através da atividade de auditoria interna, avaliar a eficácia dos procedimentos de controle inerentes ao SRH, propondo alterações na Instrução Normativa para aprimoramento dos controles.