DECRETO LEGISLATIVO Nº 3215/2020.

CONCEDE COMENDA "DR. DJALMA ELOY HESS" E DA OUTRAS PROVIDÊNCIAS.

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

RESOLVE:

Art. 1º – Fica concedida a **Comenda "Dr. Djalma Eloy Hess",** nos termos da Resolução Nº 377/2019 à:

FIORAVANTE CYPRIANO NETO
MARIO MARABOTI
VALDEIR SANTANA SPEROTTO

Art. 2º - Este Decreto entrará em vigor na data de sua publicação, revogadas as disposições em contrário.

Cachoeiro de Itapemirim-ES, 09 de novembro de 2020.

ALEXON SOARES CIPRIANO
Presidente

DECRETO LEGISLATIVO Nº 3216/2020.

CONCEDE "HOMENAGEM ESPECIAL" E DÁ OUTRAS PROVIDÊNCIAS.

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

RESOLVE:

Art. 1º – Fica concedido, nos termos da Resolução nº 066/2003, **"Homenagem Especial"** ao Professor de Educação Física:

RODOLFO PICOLE BLUNCK

Art. 2º - Este Decreto entrará em vigor na data de sua promulgação, revogadas as disposições em contrário.

Cachoeiro de Itapemirim-ES, 09 de novembro de 2020.

ALEXON SOARES CIPRIANO
Vereador - Presidente

PORTARIA Nº 354/2020

STI - SISTEMA DE TECNOLOGIA DA INFORMAÇÃO - STI n° 1/2015 – VERSÃO 02.

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 STI nº 01/2015 – versão 02, conforme anexo I.

Art. 2º – Esta Portaria entrará em vigor na data de sua publicação.

Cachoeiro de Itapemirim-ES, 05 de novembro de 2020.

ALEXON SOARES CIPRIANO
Presidente

ANEXO I

INSTRUÇÃO NORMATIVA STI Nº. 001/2015 - versão 02

SIGLAS DE REFERÊNCIA:

UCCI – Unidade Central de Controle Interno;
STI – Sistema de Tecnologia da Informação;
CMCI – Câmara Municipal de Cachoeiro de Itapemirim – E.S.;
DTI – Departamento de Tecnologia da Informação;

Versão: 2.0

Unidade Responsável: Departamento de Tecnologia da Informação

I – FINALIDADE

A presente Instrução Normativa tem por objetivo disciplinar os procedimentos administrativos do STI quanto à 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 abrange diretamente todos os setores e gabinetes desse Poder Legislativo Municipal, incluindo gabinetes dos Vereadores, e indiretamente todos os usuários de T.I. das unidades da Estrutura Organizacional, 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 espécie, 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, munícipe 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 e gabinetes que utilizem 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 colocá-las sob processamento eletrônico. Já para TURBAN (2003), os dados 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 sequência 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 início 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

1 –Constituição Federal de 1988;

2 - Lei Federal 9609/1998;

3 – Lei Federal 13709/2018;

4 – Norma ISO 27001;

5 – Demais legislações pertinentes;

V – RESPONSABILIDADES

1 – Unidade Responsável pela Instrução Normativa:

a. Promover a divulgação da Instrução Normativa, mantendo-a atualizada; Orientar as áreas executoras e supervisionar a sua aplicação;

b. 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;

2 – Unidades Executoras:

2.1 Atender as solicitações da unidade responsável pela Instrução Normativa, quanto ao fornecimento de informações e à participação no processo de atualização;

2.2 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;
2.3 Manter a Instrução Normativa à disposição de todos os usuários da Unidade, velando pelo fiel cumprimento da mesma;
2.4 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 – Unidade Responsável pela Coordenação do Controle Interno

3.1 – Prestar apoio técnico por ocasião das atualizações da Instrução Normativa, em especial no que tange à identificação e avaliação dos pontos de controle e respectivos procedimentos de controle;
3.2 – Através da atividade de auditoria interna, avaliar a eficácia dos procedimentos de controle inerentes ao STI, propondo alterações na Instrução Normativa para aprimoramento dos controles;

VI – PROCEDIMENTOS

1 – Obrigações e Permissões dos Usuários:

1.1 Para utilizar os computadores, internet, rede corporativa da CMCI, softwares, aplicativos e pastas em geral, o usuário deverá solicitar no ato da sua nomeação, à chefia imediata, a abertura de uma conta de acesso (login) e senha;
1.2 O formulário "TERMO DE RESPONSABILIDADE" (formulário 01) estará disponível no R.H. desta Casa, o qual será preenchido e assinado pelo Responsável pelo Setor, ou pelo respectivo Vereador (no caso dos gabinetes), no ato da apresentação dos documentos necessários à nomeação;
1.3 Nos casos de demissão, exoneração, aposentadoria ou qualquer outro que implique o desligamento do usuário do Poder legislativo, o departamento de RH deverá comunicar imediatamente, por escrito, o fato ao DTI para que este proceda à imediata desabilitação do usuário;
1.4 Nos casos de transferência de local de trabalho, o chefe imediato do usuário deverá comunicar imediatamente o fato à DTI, por escrito;
1.5 Toda conta de acesso é atribuída a 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;
1.6 O descumprimento do Termo de Responsabilidade (Formulário 01), caracteriza infração funcional, podendo ocasionar a responsabilização administrativa, civil e penal do infrator;
1.7 O perfil de acesso dos usuários aos aplicativos e aos sistemas será o necessário para o desempenho de suas atividades;
1.8 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;
1.9 Uma senha segura deverá conter no mínimo seis (06) caracteres alfanuméricos (letras e números) com diferentes caixas. As senhas terão um tempo de vida útil pré-determinado pelo DTI, devendo o mesmo ser respeitado, caso contrário o usuário ficará sem acesso aos serviços de rede;
1.10 As contas inativas por mais de sessenta (60) dias serão desabilitadas. O usuário que pretenda preservar seus dados deverá comunicar seu afastamento com antecedência;
1.11 As contas de acesso dos prestadores de serviços e servidores temporários deverão ser automaticamente bloqueadas na data de término de contrato;

2 – Estações de Trabalho e Componentes:

2.1 – 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;
2.2 – Caberá aos usuários comunicar imediatamente à Administração quaisquer problemas que venham ocorrer, bem como relatar qualquer suspeita de uso inadequado dos recursos computacionais;
2.3 – Não será permitido aos usuários alterar, configurar ou remanejar estações de trabalho e periféricos de seus locais de instalação sem o conhecimento do DTI;
2.4 - Não deverão ser conectados Notebooks, Laptops, Tablets ou outros equipamentos aos computadores da CMCI sem o conhecimento da DTI;
2.5 – 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;
2.6 – É vedada a abertura de computadores para qualquer tipo de reparo, cabendo exclusivamente ao DTI a realização desta atividade;
2.7 – Algumas configurações de desktop (papel de parede, opções de menu, configurações, etc.) poderão ser controladas e padronizadas pelo DTI;
2.8 – 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;
2.9 – 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;
2.10 – Não será permitida a utilização dos recursos computacionais para benefício próprio ou de terceiros, direto ou indireto, sujeitando-se o infrator à imediata suspensão de sua chave de acesso, sem prejuízo da aplicação das demais penalidades cabíveis;
2.11 – 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;
2.12 – 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;
2.13 – 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;
2.14 – 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);

3 – Ambiente de Rede:

3.1 – 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;
3.2 – É expressamente proibido o uso de meios ilícitos de acesso aos computadores, sistemas e arquivos do ambiente de rede computacional da CMCI;
3.3 – É proibido o acesso remoto aos computadores da rede da CMCI sem o conhecimento e subsequente autorização do DTI;
3.4 – 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;
3.5 – Não será permitida a alteração das configurações de rede e do sistema das máquinas, bem como modificações que possam trazer algum problema futuro;
3.6 – É expressamente proibido tentar burlar a utilização dos recursos computacionais da CMCI, com o objetivo de obter proveito pessoal ou violar sistemas de segurança estabelecidos;
3.7 – Os usuários não poderão instalar ou fazer "upgrade" de qualquer espécie de programas ou aplicativos na estação de trabalho sem aprovação do DTI;
3.8 – 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;
3.9 – 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;

4 – Correio Eletrônico Institucional (e-mail)

4.1 – O acesso ao sistema de correio eletrônico será disponibilizado aos usuários com necessidade manifesta de usá-lo como ferramenta de apoio às atividades profissionais, podendo ocasionalmente ser utilizado para mensagens pessoais curtas e pouco frequentes;
4.2 – 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;
4.3 – 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;
4.4 – Não será permitido o uso de endereços de e-mail para troca de informações ligadas a práticas que infrinjam qualquer lei nacional ou internacional;
4.5 – O usuário não deverá abrir e-mails com arquivos anexados quando não conhecer o remetente, sob o risco de estar infectando com vírus o seu equipamento;

5 – Internet:

5.1 – O uso de internet deverá ser controlado e restrito às atividades profissionais, no sentido de manter os mais altos níveis de qualificação em prol da atualização da informação;
5.2 – É vedado utilizar-se dos serviços internos de internet da CMCI desviando-se de sua finalidade, com o intuito de cometer fraudes;
5.3 – É vedado 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;
5.4 – Não será permitido acessar salas de bate-papo (chat rooms), jogos, apostas e assemelhados;
5.5 – 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;
5.6 – Não será permitido fazer download de arquivos cujo conteúdo não tenha relação com as atividades realizadas pela CMCI;
5.7 – É vedada 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;
5.8 – Ficará a 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;
5.9 – O sistema de filtro de acessos, bem como o sistema de monitoramento de uso, poderão gerar relatórios solicitados pela chefia imediata indicando os usuários que eventualmente navegarem e/ou acessarem recursos da internet indevidamente, ficando desde já cientes todos os usuários do supracitado monitoramento;
5.10 – Não será permitida a utilização de software não homologado pelo DTI para ser o cliente de navegação;
5.11 – Não será permitida a manutenção não autorizada de páginas pessoais ou de serviços particulares envolvendo comercialização pela internet utilizando os recursos computacionais da CMCI;

6 – Armazenamento de Documentos e Informações:

6.1 – O usuário deverá manter sigilo sobre os documentos e informações considerados estratégicos, confidenciais ou de interesse privativo da CMCI;
6.2 – Todos os documentos e informações dos setores administrativos da CMCI deverão ser armazenados nos diretórios em pastas devidamente identificadas por departamento;
6.3 – O usuário deverá informar ao seu superior imediato quando informações ou aplicações consideradas estratégicas ou confidenciais forem encontradas sem o tratamento de segurança correto;
6.4 – 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;
6.5 – 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;

7 – Advertências e Penalidades:

7.1 – Os usuários deverão estar cientes das regras e normas de uso dos recursos computacionais evitando deste modo a utilização indevida dos mesmos;
7.2 – 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;
7.3 – 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;

8 – Responsabilidades do Departamento de Tecnologia da Informação:

8.1 – 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;
8.2 – 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;
8.3 – 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;
8.4 – 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;
8.5 – 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;
8.6 – 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;
8.7 – 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;
8.8 – No tocante à 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;

9 – Responsabilidades das Unidades Usuárias dos Recursos Computacionais:

9.1 – 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;
9.2 – Definir os níveis de acesso (consulta/atualização) aos, sistemas, rotinas/programas, arquivos e dados, para todos os aplicativos de responsabilidade de sua área;
9.3 – 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;
9.4 – Fazer a utilização do produto de antivírus de acordo com as instruções recebidas do DTI;
9.5 – 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 sobre as rotinas e procedimentos relacionadas a esta Instrução Normativa poderão ser obtidos junto ao DTI.

3 – A inobservância das normas estabelecidas nesta Instrução Normativa pelos agentes públicos poderá acarretar 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.

Cachoeiro de Itapemirim – E. S. 29 de outubro de 2020.

Departamento de Tecnologia da Informação
RONALDO CRUZ GARCIA JUNIOR
Supervisor de Informática – MATRÍCULA CMCI 1012

INSTRUÇÃO NORMATIVA STI Nº. 001/2015 – Versão 02

Formulário 01

Departamento de Tecnologia da Informação

Termo de Responsabilidade

Eu, _____, declaro haver solicitado acesso à rede de computadores interna dessa Casa de Leis bem como seus recursos acessórios, comprometendo-me a utilizá-lo(s) conforme a IN STI 01 e 02 /2015 na sua última versão, disponível em https://www.transparencia.cachoeirodeitapemirim.es.leg.br/transparencia/legislacao/especie/13/sti-sistema-de-tecnologia-da-informacao, a qual confirmo ter lido nessa data.

Cachoeiro de Itapemirim-ES, _____ de _____ de _____.

_____
Usuário