INSTRUÇÃO NORMATIVA Nº 001/2015

DISPÕE SOBRE PROCEDIMENTOS PARA SEGURANÇA FÍSICA E LÓGICA DOS EQUIPAMENTOS, SISTEMAS, DADOS E INFORMAÇÕES.

VERSÃO: 01

DATA: 23/09/2015

ATO DE APROVAÇÃO: DECRETO Nº 539/2015

UNIDADE RESPONSÁVEL:

DIRETOR TÉCNICO DE DESENVOLVIMENTO DE TECNOLOGIA DA INFORMAÇÃO DA SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO.

CAPÍTULO I
DA FINALIDADE

Art. 1 - A presente Instrução dispõe sobre "Procedimentos para Segurança Física e Lógica dos Equipamentos, sistemas, dados e Informações", objetivando a implementação de rotinas de trabalho e de procedimentos de controle.

CAPÍTULO II
DA ABRANGÊNCIA

Art. 2 - Abrange todas as unidades da estrutura administrativa do município, no âmbito da operacionalização dos Procedimentos do Sistema de Tecnologia da Informação e aplica-se a todos os usuários de recursos de tecnologia da informação, quer como executoras de tarefas, quer como fornecedoras ou recebedoras de dados e informações em meio documental ou informatizado, que deverão observar, a legislação municipal, estadual, federal e os procedimentos constantes desta Instrução Normativa.

CAPÍTULO III
DOS CONCEITOS

Art. 3 - Para os fins desta Instrução Normativa considera-se:

I- Instrução Normativa: documento que estabelece os procedimentos a serem adotados objetivando a padronização na execução de atividades e rotinas de trabalho que devem processar de forma constante e periódica.

II- Manual de rotinas Internas e Procedimentos de Controle: coletânea de Instruções Normativas que tem por objetivo veicular as informações necessárias à execução das atividades.

III- Recursos Tecnológicos: os equipamentos, as instalações e bancos de dados direta ou indiretamente administrados, mantidos ou operados pelas diversas secretarias, órgãos, diretorias, Coordenadorias e Gerências, tais como:

a) Computadores (Desktop ou Notebook), incluídos seus equipamentos: CD's/DVD´s, pen drive e acessórios;
b) Impressoras, plotters e equipamentos multifuncionais conectados ao computador;
c) Redes de computadores e de transmissão de dados;
d) Bancos de dados ou documentos residentes em disco, fita magnética ou outros meios;
e) Leitores de códigos de barra, scanners, equipamentos digitalizadores e afins.
f) Manuais técnicos e CD's/DVD´s de instalação/configuração;
g) Patch panel, switches, hubs, appliance e outros ativos de rede;
h) Serviços e informações disponibilizados via arquitetura de informática da instituição;
i) Softwares, sistemas e programas adquiridos ou desenvolvidos pela Administração.

IV – Usuário: todo servidor público municipal ou prestador de serviço que necessite de acesso à rede corporativa ou utilize algum recurso de tecnologia da informação municipal;

V – Cadastro: procedimento de criação de usuário para acesso aos sistemas informatizados da Prefeitura Municipal;

VI – Habilitação: procedimento de atribuição dos módulos ao usuário;

VII – Módulo: subconjunto de transações de um sistema, que define a abrangência de atuação de um usuário;

VIII – Senha: conjunto alfanumérico de caracteres destinado a assegurar a identidade do usuário e permitir seu acesso aos dados, programas e sistemas não disponíveis ao público, de uso pessoal e intransferível;

IX – Ativos de Informação: o patrimônio composto por todos os dados e informações gerados e manipulados nos processos do órgão;

X – Ativos de Processamento: patrimônio composto por todos os elementos de hardware (máquina), software (sistema) e infraestrutura de comunicação, necessários para a execução das atividades do órgão;

XI – Recursos de Tecnologia da Informação: conjunto dos ativos de informação e de processamento;

XII – Dado: qualquer elemento identificado em sua forma bruta que por si só não conduz a uma compreensão de determinado fato ou situação, constituindo um insumo de um sistema de informação;

XIII – Informação: resultado do processamento do conjunto de dados apresentados a quem de direito, na forma, tempo e meio adequado, que permite conhecer uma avaliação ou fato, contribuindo para a tomada de decisão;

XIV – Informações Íntegras: aquelas que apenas são alteradas através de ações autorizadas e planejadas;

XV – Informações Integradas: aquelas que fazem parte de um todo que se completam ou complementam;

XVI – Sistema de Informação: conjunto de partes que formam um todo unitário, com o objetivo de disciplinar informações para formular, atingir e avaliar as metas da organização;

XVII - Tecnologia da Informação: conjunto de equipamentos e suportes lógicos que visam coletar, processar, tratar, armazenar e distribuir dados e informações;

XVIII – Confidencialidade: o princípio de segurança que trata da garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

XIX – Integridade: o princípio de segurança que trata da salvaguarda da exatidão e confiabilidade da informação e dos métodos de processamento;

XX – Disponibilidade: o princípio de segurança que trata da garantia de que pessoas autorizadas obtenham acesso à informação e aos recursos correspondentes, sempre que necessário;

XXI – Segurança da Informação: a preservação da confidencialidade, integridade, credibilidade e disponibilidade da informação, adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade podem estar envolvidas;

XXII – Credencial: a combinação do “login” e “senha”, utilizado ou não em conjunto a outro mecanismo de autenticação que visa legitimar e conferir autenticidade ao usuário na utilização da infraestrutura e recursos de informática;

XXIII – Suporte Técnico: serviço realizado pela equipe da Diretoria Técnica de Desenvolvimento da Tecnologia da Informação que tem a responsabilidade de dar suporte às ações do sistema da Tecnologia da Informação.

CAPÍTULO IV
DA BASE LEGAL

Art. 4 - O fundamento jurídico encontra-se respaldado na:

I – Constituição Federal;

II – NBR ISSO/IEC 17799;

CAPÍTULO V
DAS RESPONSABILIDADES

Art. 5 - São responsabilidades da diretoria Técnica de Desenvolvimento da Tecnologia da Informação enquanto Unidade Responsável pela Instrução Normativa:

I – Promover discussões técnicas com as unidades executoras e com a Unidade Central de Controle interno, para definir as rotinas de trabalho e identificar os pontos de controle e respectivos procedimentos de controle, objetos da Instrução Normativa a ser elaborada;
II – Obter a aprovação da Instrução Normativa, após submetê-la à apreciação da Unidade de Controle Interno e promover sua divulgação e implementação;
III – Manter atualizada, orientar as áreas executoras e supervisionar a aplicação da Instrução Normativa;
IV – Potencializar o uso da informação e da tecnologia da informação no cumprimento da missão do município;
V – Subsidiar com informações necessárias e suficientes o processo de tomada de decisão da Administração Pública;
VI – Disponibilizar informações que possibilitem à Administração Pública o atendimento das necessidades do cidadão;
VII – Possibilitar qualidade e transparência às ações de governo permitindo um melhor controle social;
VIII – Promover a evolução, de forma coordenada, dos assuntos relacionados à informação e tecnologia da informação no âmbito da Administração Pública Municipal, visando a melhoria do desempenho das pessoas nos processos da organização;
IX- Promover a sinergia das ações da Administração Pública no intuito de propiciar a inclusão digital;
X – Promover o livre intercâmbio de informações e conhecimentos com a sociedade, contribuindo para o seu desenvolvimento;
XI – Propiciar a melhoria da gestão pública, contribuindo para a produção de resultados que promovam a justiça social;
XII – Coordenar no âmbito do Governo as ações do governo eletrônico;
XIII – Analisar periodicamente a efetividade da política de Segurança da Informação, propondo mecanismos institucionais para melhoria contínua bem como assessorar, em matérias correlatas, as demais unidades da Administração Municipal;
XIV – Avaliar as mudanças importantes na exposição dos recursos a riscos, identificando as principais ameaças;
XV – Analisar criticamente os incidentes de Segurança da Informação e ações corretivas correlatas.
XVI – Promover o aprimoramento dos procedimentos de controle e o aumento da eficiência operacional;
XVII – Manter a Instrução Normativa à disposição de todos os funcionários da unidade, velando pelo fiel cumprimento da mesma;
XVIII – 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;
XIX – Conscientizar os usuários internos e colaboradores sob sua supervisão em relação aos conceitos e as práticas de segurança da informação;

XX – Incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à segurança da informação;
XXI – Comunicar ao superior imediato e a unidade competente em caso de comprometimento da segurança e quaisquer outras faltas, desvios ou violação das regras estabelecidas para adoção de medidas cabíveis.

Art. 6 - São responsabilidades da Unidade de Controle Interno – UCI:

I – Prestar o apoio técnico na fase de elaboração das Instruções Normativas e em suas atualizações, em especial no que tange à identificação e avaliação dos pontos de controle e respectivos procedimentos de controle;
II – Através da atividade de auditoria interna, avaliar a eficiência dos procedimentos de controle inerentes a cada sistema administrativo, propondo alterações nas Instruções Normativas para aprimoramento dos controles ou mesmo a formatação de novas Instruções Normativas;
III – Organizar e manter atualizado o manual de procedimentos, em meio documental e/ou em base de dados, de forma que contenha sempre a versão vigente de cada Instrução Normativa.

CAPÍTULO VI
DOS PROCEDIMENTOS

Seção I
Das obrigações e permissões dos usuários

Art. 7 - A política de Segurança da informática se aplica a todos aqueles que exerçam, ainda que transitoriamente e sem remuneração, por nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, cargo, emprego ou função pública no âmbito da administração municipal e que façam uso de seus recursos materiais e tecnológicos.

Art. 8 - A fim de resguardar a continuidade, integridade, credibilidade e disponibilidade das informações e serviços, devem ser adotados mecanismos de proteção.

Art. 9 –Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela Prefeitura Municipal é considerada de sua propriedade e deve ser protegida, de acordo com esta Instrução Normativa.

Art. 10 – As informações devem ser classificadas de acordo com um sistema próprio, determinado pela necessidade de sigilo, confidencialidade e disponibilidade, para garantir o armazenamento, a proteção de acesso e o uso adequado.

Art. 11 – Os sistemas e equipamentos utilizados para armazenamento de informações devem receber a mesma classificação dada a informação neles mantida.

Art. 12 – Deverão ser realizadas auditorias periódicas dos ativos, de forma a aferir o correto cumprimento da Política de segurança da informação.

Art. 13 – Fica assegurado ao Suporte Técnico, de ofício ou a requerimento do responsável pela unidade administrativa, necessariamente referendado pelo Secretário da pasta, a qualquer tempo, a competência de suspender temporariamente o acesso do usuário a recurso de tecnologia da informação da prefeitura, quando evidenciados riscos à segurança da informação.

Art. 14 – Caberá conjuntamente ao Diretor Técnico e Controle Interno, elaborar, revisar, atualizar, divulgar e validar as diretrizes, normas, procedimentos e instruções, que regulamentem os princípios e valores existentes na Política de Segurança da Informação, visando à regulamentação e operacionalização das diretrizes apresentadas nesta Instrução Normativa.

Art. 15 – As normas e procedimentos de que trata esta Instrução Normativa deverão ser elaboradas tomando-se por base os objetivos e controles estabelecidos na ABNT NBR ISSO/TEC 17799, quais sejam:

I – Organização da segurança da informação;
II – Gestão de ativos;
III – Segurança em recursos humanos;
IV- Segurança física e do ambiente;
V – Gerenciamento das operações e comunicações;
VI – Controles de acessos;
VII – Aquisição, desenvolvimento e manutenção de sistemas de informação;
VIII – Gestão de incidentes de segurança da informação;
IX – Gestão da continuidade do negócio;
X – Conformidade.

Art. 16 – Todos os recursos de tecnologia da informação da Prefeitura devem ser inventariados, classificados, atualizados periodicamente e mantidos em condição de uso.

Art. 17 - Cada recurso de tecnologia da informação deverá ter um gestor formalmente designado.

Art. 18 – Deverá ser implementado processo de gerenciamento de riscos, visando a identificação e à mitigação dos mesmos, associados às atividades críticas da Prefeitura.

Art. 19 – Deverão ser elaborados planos de continuidade de negócio para cada atividade crítica de forma a garantir o fluxo das informações necessárias em momento de crise e o retorno seguro à situação de normalidade.

Art. 20 – Deverão ser realizados procedimentos de salvaguarda de informações, em local externo à Sala de Informática, através de backup periódico no mínimo semanal, para salvaguardar as bases de dados dos sistemas da prefeitura.

Seção II
Das contas de acesso (login)

Art. 21 – Para utilizar os computadores e obter acesso ao correio eletrônico, internet da rede corporativa do Município, software, aplicativos e pastas em geral, o secretário da pasta na qual o servidor está vinculado, deverá solicitar ao suporte Técnico, através a abertura de uma conta de acesso (login) e senha para o servidor, quando de sua admissão.

Art. 22 – O credenciamento de usuários e efetivação das permissões será realizado pelo Suporte Técnico por meio de solicitação através do sistema de abertura de chamado disponível na Intranet do município.

Art. 23 – As contas de acesso aos recursos de Tecnologia de Informação terão a seguinte padronização:
I – Para os casos de e-mail Institucional Pessoal (Primeiro nome) (último sobrenome) @ Guarapari.es.gov.br;
II – Para os casos de e-mail Institucional Gerencial será por meio de lista de distribuição (nome da Gerência)@guarapari.es.gov.br.

Art. 24 – O e-mail institucional gerencial será utilizado pelo superior responsável da respectiva Gerência ou a quem por ele for designado, para fins de comunicação com outros órgãos e entidades, com o objetivo de centralizar as informações estratégias da Secretaria em um único e-mail.

Art. 25 – A forma de utilização dos e-mails institucionais seguirá rigorosamente esta Instrução Normativa.

Art. 26 – O Suporte Técnico terá 30 (trinta) dias após a aprovação desta Instrução Normativa para solicitar a lista dos servidores efetivos e a lista de todos os setores à Gerência de Recursos Humanos, para que se efetue a padronização de todos os endereços de e-mails desta Prefeitura.

Art. 27 – Anualmente, no mês de fevereiro, o suporte Técnico deverá atualizar e divulgar a todos os setores da Prefeitura a lista de todos os servidores e seus respectivos e-mails institucionais.

Art. 28 – Ao receber a conta de acesso, o usuário e/ou colaborador deverá assinar e cientificar o Termo de Responsabilidade de Utilização de recursos de tecnologia da informação da Prefeitura, conforme ANEXO I.

Art. 29 – Mudança de lotação, atribuições, afastamento definitivo ou temporário do usuário, deverão ser automaticamente comunicados ao suporte Técnico pelo Secretário da pasta, para procedimentos de ajustes ou cancelamento de conta de acesso, cabendo a este secretário o ônus por qualquer uso indevido da credencial do usuário decorrente da não comunicação de algum dos eventos tratados neste item.

Art. 30 – 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.

Art. 31 - Os usuários não deverão colocar objetos sobre os equipamentos de forma a prejudicar o seu sistema de ventilação, assim como manipular líquidos, alimentos ou substâncias que possam ocasionar danos quando os estiver operando.

Art. 32 – O usuário deverá encerrar sua sessão (desligar ou fazer logoff) na estação de trabalho ao término de suas atividades, sendo que, ao final do expediente a estação de trabalho deverá ser desligada.

Art. 33 – Os usuários devem alterar suas senhas iniciais no primeiro acesso, sendo responsáveis por todas as ações realizadas mediante os logins e senhas que lhe são atribuídos.

Seção III

Softwares, Hardwares e Impressoras

Art. 34 – De forma a zelar pela segurança do seu computador, sempre que o programa de antivírus enviar mensagem informando que algum arquivo está infectado por vírus, o usuário deverá informar imediatamente ao Suporte Técnico.

Art. 35 – Todo Software existente no parque computacional da prefeitura precisa estar licenciado e quando não, ser classificado como OpenSource (Software de uso livre).

Art. 36 – Toda instalação de Software deverá ser realizada pela equipe de Suporte Técnico.

Art. 37 – É proibida a transferência de qualquer tipo de programa, jogo, e similares, para a rede interna da Prefeitura.

Art. 38 – É proibido o uso de jogos inclusive os da internet (online);

Art. 39 – É vedada a abertura de computadores, para qualquer tipo de reparo. Quando houver necessidade de reparo, deve se abrir um chamado através da INTRANET ou por telefone na falta deste.

Art. 40 – Não é permitida a alteração das configurações de rede.

Art. 41 – Todo software instalado nos computadores, por padrão, é de posse da instituição, sendo vedada a cópia, clone, uso de licença ou qualquer outra forma de disponibilizá-los a terceiros.

Art. 42 – Não é permitida a remoção dos softwares padrão instalados nos computadores.

Art. 43 – Não é permitida a instalação de outro software de antivírus que não seja o padrão adotado pelo Órgão/Entidade.

Art. 44 – Se a impressão sair errada, e o papel puder ser reaproveitado, deve ser recolocado na bandeja de impressão. Quando o papel não puder ser reaproveitado, verificar se pode ser usado como rascunho ou se deve ser descartado.

Art. 45 – Se a impressora emitir alguma folha em branco, esta deve ser recolocada na bandeja.

Art. 46 – Quando a quantidade de papel, na bandeja das impressoras, estiver no final, providenciar o reabastecimento, evitando assim problemas na impressão ou acúmulo de trabalhos na fila de impressão.

Art. 47 – Utilizar as impressoras coloridas somente para versão final de trabalhos e não para testes ou rascunhos.

Art. 48 – Todas as impressoras estarão por padrão configurados para imprimir Frente/Verso (Duplex) cabendo ao usuário a sua alteração no momento da impressão.

Seção IV
Do Ambiente de Rede

Art. 49 – O Suporte Técnico disponibilizará os pontos de rede necessários ao desenvolvimento das atividades dentro de seus prédios. Qualquer alteração ou criação de um ponto novo deverá ser comunicado num tempo hábil.

Art. 50 – É expressamente proibido o uso de meios ilícitos de acesso aos computadores, sistemas e arquivos do ambiente de rede computacional municipal.

Art. 51 – É proibido o acesso remoto aos computadores da Rede Pública Municipal sem o conhecimento ou consentimento do usuário.

Art. 52 – Não deverá ser utilizada quaisquer materiais ou informações, incluindo arquivos, textos, planilhas ou imagens disponíveis na rede corporativa do município, que não respeitem os direitos autorais, marcas registradas, patentes, sigilos comerciais ou outros direitos de propriedade intelectual de terceiros.

Art. 53 – Fica proibido tentar burlar a utilização dos recursos computacionais do Município com o objetivo de obter proveito pessoal ou violar Sistemas de Segurança estabelecidos.

Art. 54 – Fica proibido o uso de dispositivos móveis pessoais (celulares/Tablets/Notebooks) na Rede Corporativa da Prefeitura, salvo casos extremos.

Art. 55 – O uso de Redes Sem Fio (wireless) só será permitido quanto instalada e configurada pela equipe de Suporte Técnico e ainda para atender a equipamentos pertencentes a Prefeitura Municipal. O uso de roteadores pessoais é extremamente proibido.

Art. 56 – A área denominada pública (Unidade j) disponível na rede local deve:

a) ser utilizada somente para a transferência de arquivos entre usuários, não devendo ser utilizada para o armazenamento de informações;

b) ter seu conteúdo apagado pela Unidade responsável pela TIC, semanalmente, ou de acordo com a necessidade de liberação de espaço nos servidores.

Art. 57 – Os usuários devem encerrar ou bloquear a sessão da estação de trabalho sempre que se ausentarem desta.

Seção V
Do Correio Eletrônico (e-mail)

Art. 58 – O acesso ao sistema de correio eletrônico será disponibilizado aos usuários com necessidade manifesta de usá-lo como ferramenta de apoio às atividades profissionais.

Art. 59 – Não será permitido participar, criar, ou distribuir voluntariamente mensagens indesejáveis, como circulares, manifestos públicos, correntes de cartas, SPAM ou similares que possam prejudicar o trabalho de terceiros, causar tráfego na rede ou sobrecarregar os sistemas computacionais desnecessariamente.

Parágrafo único – Considera-se SPAM o envio em massa de e-mails para usuários que não os solicitaram 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.

Art. 60 – Não é permitido o uso de endereços de E-Mail para trocas de informações ligadas a práticas que infrinjam qualquer lei municipal ou internacional.

Art. 61 – O usuário não deverá abrir E-Mail com arquivos anexados quando não conhecer o remetente sob risco de estar infectando com vírus seu equipamento.

Art. 62 – Fica extremamente proibido o uso de e-mails que não sejam institucionais (@guapari.es.gov.br e/ou @guarapari-edu.com.br) para tratar de assuntos ligados a Prefeitura de Guarapari.

Art. 63 – O uso de e-mail corporativo não garante direito sobre este, nem confere autoridade para liberar acesso a outras pessoas, pois se constitui de informações pertencentes a Prefeitura.

Art. 64 – O acesso a correio eletrônico particular somente será permitido através dos navegadores de internet.

Art. 65 – Os usuários são responsáveis por manter o espaço disponibilizado para o armazenamento de mensagens na sua caixa postal, evitando sua indisponibilidade. As mensagens já lidas devem ser excluídas da Caixa de Entrada e da Lixeira.

Art. 66 – O Setor de Tecnologia poderá a qualquer tempo e sem prévio aviso suspender acesso a ferramentas de e-mail não ligadas a Prefeitura.

Seção VI
Da Internet

Art. 67 – Não é permitido ao usuário utilizar-se dos serviços internos de Internet do Município desvirtuando sua finalidade com o intuito de cometer fraudes.

Art. 68 – Não é permitido 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 incentivos a violência ou outro material que possa violar qualquer lei aplicável.

Art. 69 – Não é permitida a navegação aos sites pertencentes às categorias abaixo:

- Pornográfico e de caráter sexual;
- Compartilhamento de arquivos (ex.: peer to peer, Bit Torrent, emule, etc.);
- Pornografia infantil (pedofilia);
- Apologia ao terrorismo;
- Apologia às drogas;
- Crackers;
- De relacionamento (Badoo,Gazzag, Facebook, etc.);
- Violência e agressividade (racismo, preconceito, etc.);
- Violação de direito autoral (pirataria, etc.);
- Áudio e vídeo, salvo com conteúdo relacionado diretamente a atividades administrativas ou profissionais;
- Instant messenger;
- Conteúdo impróprio, ofensivo, ilegal, discriminatório e similares

Art. 70 – Ficará expressamente proibido utilizar ferramentas que burlam a segurança, para usufruir serviços que não lhes são concebidos.

Art. 71 – Não será permitida a manutenção não autorizada de páginas pessoais ou de serviços particulares envolvendo comercialização pela internet utilizando os recursos computacionais do Município.

Art. 72 – É proibido downloads de arquivos de extensões tipo: .exe, .mp3, .wav, .bat, .com, .sys, .scr, .ppt, .mpeg, .avi, .rmvb, .dll, e de programas de entretenimento ou jogos, salvo os estritamente relacionados aos serviços inerentes à função do servidor.

Art. 73 – Não é permitido o acesso a programas de TV na internet ou qualquer conteúdo sob demanda (streaming).

Art. 74 – 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, entre outros.

Art. 75 – Acessos as Redes Sociais só serão permitidas mediante aprovação do superior responsável da respectiva Gerência.

Seção VII

Da assistência técnica aos recursos computacionais

Art. 76 – Qualquer problema nos recursos computacionais da instituição deverá ser comunicado pelo responsável do recurso computacional ao Suporte técnico através da ferramenta on-line de abertura de chamados localizações na INTRANET, SITE NA INTERNET ou ainda através do telefone de suporte.

Art. 77 – O técnico do suporte Técnico deverá atender ao Chamado de Assistência Técnica em até 48 (quarenta e oito) horas da abertura do chamado.

Art. 78 – O técnico do Suporte Técnico terá o prazo de 72 (setenta e duas) horas, a partir do atendimento inicial, para apresentar solução ao Chamado de Assistência Técnica em Informática, sob pena de ser considerado "concluído Fora do Prazo", para fins de avaliação da eficiência e eficácia do departamento.

Art. 79 – Para casos onde sejam necessário deslocamento do técnico, o Setor que faz o requerimento de Suporte Técnico deverá fornecer o transporte para buscar e retornar com o técnico para seu local de origem.

Art. 80 – Para todo atendimento de Suporte Técnico é necessário ter um chamado em aberto ficando vetado ao Técnico o atendimento sem o mesmo.

Seção VIII

Do armazenamento de documentos e informações

Art. 81 – O usuário deverá manter sigilo sobre os documentos e informações considerados estratégicos, confidenciais ou de interesse particular da Administração Pública Municipal.

Art. 82 – Os documentos e informações considerados estratégicos ou confidenciais deverão ser armazenados nos diretórios pessoais em pasta devidamente identificada por Secretaria.

Parágrafo único – A classificação de um documento como "confidencial" resulta da comunicação por escrito do secretário da pasta aos servidores, desde que seja fundamentado o motivo da exceção ao princípio da publicidade.

Art. 83 – O usuário deverá informar ao seu superior imediato quando informações ou aplicações consideradas estratégicas ou confidenciais forem encontradas sem o tratamento de segurança correto.

Art. 84 – O unidade C: não deverá ser utilizado pelo usuário para guardar documentos importantes ou confidenciais, sob o risco de perdê-los a qualquer tempo.

Art. 85 – Os documentos deverão ser salvos em unidade de rede mapeadas em sua estação e/ou na unidade D de seu equipamento quando houver.

Art. 86 – Os documentos e informações geradas pelos usuários referentes às rotinas de trabalho no que diz respeito a alterações, gravações e leituras, são de inteira responsabilidade dos usuários do arquivo.

Seção IX

Das advertências e penalidades

Art. 87 – Os usuários deverão estar cientes das regras e normas de uso dos recursos computacionais, evitando, desse modo, os procedimentos que prejudicam ou impedem outras pessoas de terem acesso a esses recursos ou de usá-los de acordo com o que é determinado.

Art. 88 – 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 ao seu superior imediato, ao controle Interno e/ou ao Técnico do Suporte Técnico;

Art. 89 – Sempre que julgar necessário para a preservação da integridade dos recursos computacionais e segurança da informação ou em caso de constatação e identificação de não conformidade às normas, o Suporte Técnico fará imediatamente o bloqueio temporário da conta de acesso e comunicará o superior imediato o teor da infração e o nome do responsável para que sejam tomadas as medidas cabíveis para a apuração dos fatos.

Art. 90 – A liberação da conta de acesso somente poderá ser autorizada pelo superior imediato da pasta.

Art. 91 – Caso a violação de alguma norma for passível de aplicação de penalidade além das aqui determinadas, incluindo as situações consideradas graves ou reincidentes, o caso será apurado mediante a instauração de Processo de Sindicância, podendo derivar para Processo Administrativo Disciplinar, considerando que, sempre que tiver ciência de irregularidade no Serviço Público, acha-se obrigada a autoridade competente de promover a sua apuração imediata.

Seção X
Das Disposições Gerais

Art. 92 – Todos os certificados de autenticidade, chaves de acesso, chaves seriais de softwares, mídias de instalação e demais documentos inerentes aos aspectos dos recursos de informática, devem ficar sob responsabilidade da Secretaria de Administração, a qual disponibilizará às equipes de Controladoria Interna e externa, quando solicitados.

Art. 93 – O possível desconhecimento dessas normas por parte do usuário não o isenta das responsabilidades e das sanções aplicáveis nem poderá minimizar as medidas cabíveis.

Art. 94 – Os casos omissos e não previstos nesta Norma Interna deverão ser tratados junto à Secretaria Municipal de Administração e ao Controle Interno.

CAPÍTULO VII
Considerações Finais

Art. 95 – O descumprimento do previsto nos procedimentos aqui definidos será objeto de instauração de sindicância e de processo administrativo disciplinar para apuração da responsabilidade da realização do ato contrário às normas instituídas.

Art. 96 – Os esclarecimentos adicionais a respeito deste documento poderão ser obtidos junto à Unidade Responsável pelo Sistema, e junto à Unidade de Controle Interno – UCI que, por sua vez, através de procedimentos de auditoria Interna, aferirá a fiel observância de seus dispositivos por parte das diversas unidades da estrutura organizacional.

Art. 97 – Esta instrução entra em vigor a partir da data de sua aprovação e publicação.

Guarapari, 23 de setembro de 2015.

_____

RITA DE CÁSSIA NOSSA DE ALMEIDA

Controladoria Geral do Município

_____

CLAUDINEY ALVES

Diretor Técnico de Desenvolvimento da Tecnologia Da Informação

ANEXO I

TERMO DE RESPONSABILIDADE DE UTILIZAÇÃO DE ATIVOS E RECURSOS DE INFORMÁTICA

SECRETARIA:
SETOR:
COMPUTADOR PLAQUETA Nº:
MONITOR PLAQUETA Nº:
Nome do Responsável:
E-Mail institucional:
Matrícula:

Eu, _____, pelo presente instrumento, na condição de servidor da Prefeitura Municipal de Guarapari, comprometo-me a cumprir todas as orientações e determinações especificadas na Instrução Normativa Nº 01/2015 e outras editadas, em função do vínculo jurídico e funcional que tenho com o Município de Guarapari, bem como as informações pertencentes à Instituição, ou por ela custodiadas, em razão da permissão de acesso aos recursos necessários para a execução de minhas atividades profissionais, estando ciente, de acordo, aderente e responsável que devo obedecer, cumprir e respeitar as políticas, diretrizes, normas e procedimentos de Segurança da Informação da Prefeitura Municipal de Guarapari, publicadas e armazenadas nos meios de comunicação internos que regem o uso dos recursos a mim disponibilizados, sejam estes digitais ou impressos, bem como o manuseio das informações a que tenho acesso, ou possa vir a ter, em decorrência da execução de minhas atividades profissionais.

Manifesto conhecimento de que descumprindo os compromissos por mim assumidos neste Termo estarei sujeito às sanções aplicáveis.

Guarapari, ____ de _____ de _____

_____
Assinatura do servidor