



INSTRUÇÃO NORMATIVA STI Nº 001/2016

Dispõe sobre os procedimentos para segurança física e lógica dos equipamentos, sistemas, dados e informações do Poder Executivo do Município de Itarana/ES.

Versão: 01.

Aprovação em: 17/11/2016

Ato de aprovação: Decreto nº 786/2016

Unidade Responsável: Secretaria Municipal de Administração e Finanças – SEMAF.

CAPÍTULO I DA FINALIDADE

Art. 1º Esta Instrução Normativa tem por finalidade disciplinar e normatizar procedimentos para a segurança física e lógica dos equipamentos, sistemas, dados e informações do Poder Executivo do Município de Itarana/ES.

CAPÍTULO II DA ABRANGÊNCIA

Art. 2º Esta Instrução Normativa abrange toda a estrutura organizacional da Prefeitura de Itarana/ES no diz respeito à operacionalização dos procedimentos do sistema de tecnologia da informação aplicando-se aos usuários dos recursos de tecnologia da informação, quer como executora de tarefas quer como fornecedoras ou receptoras de dados e informações em meio documental ou informatizado, que deverão observar, além desta Instrução, as legislações municipal, estadual e federal.

CAPÍTULO III CONCEITOS

Art. 3º 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;

II – Sistema de Controle Interno – SCI: Conjunto de procedimentos de controle estruturados por diversos sistemas administrativos e especificados em Instruções Normativas, executados ao longo de toda a estrutura organizacional, sob a coordenação, orientação técnica e supervisão da unidade responsável pela coordenação do controle interno;

III – Unidades Executoras: Todas as Secretarias e respectivas unidades da estrutura organizacional do Poder Executivo do Município de Itarana/ES, no exercício das atividades de controle interno inerentes às suas funções finalísticas ou de caráter administrativo;

IV – Servidor Público: Pessoa legalmente investida em cargo, emprego ou função pública, vinculada à Administração Pública Municipal sob o regime jurídico estatutário, especial ou celetista;

V – Recursos Tecnológicos: Os equipamentos, as instalações e bancos de dados direta ou indiretamente administrados, mantidos ou operados pelos diversos órgãos da estrutura organizacional da Prefeitura.

São eles:

a) computadores, incluídos seus softwares e *hardwares*, *pen drives* e acessórios como: impressoras, *plotters*, equipamentos multifuncionais leitoras de códigos de barra, scanners, equipamentos digitalizadores e afins;

b) redes de computadores e de transmissão de dados;

c) bancos de dados ou documentos residentes em disco, fita magnética ou outros meios;

d) serviços e informações disponibilizados via arquitetura de informática da instituição;

e) sistemas e programas adquiridos ou desenvolvidos pela Administração;

f) *patch panel*, *switches*, *hubs* e outros equipamentos de rede;

g) manuais técnicos e CD's de instalação/configuração.

VI – Usuário: Todo servidor público municipal ou prestador de serviço que necessite de acesso à rede corporativa ou utilize algum recurso de tecnologia da informação do município;

VII – Cadastro: Procedimento de criação de usuário para acesso aos sistemas informatizados da Prefeitura;

VIII – Habilitação: Procedimento de atribuição dos módulos ao usuário;

IX – Módulo: Subconjunto de transações de um sistema, que define a abrangência de atuação de um usuário;

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

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

XII – Ativos de Processamento: Patrimônio composto por todos os elementos de *hardware*, *software* e infraestrutura de comunicação necessários para a execução das atividades do órgão;

XIII – Recursos de Tecnologia da Informação: Conjunto dos ativos de informação e de processamento;

XIV – 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;

XV – Informação: Resultado do processamento do conjunto de dados apresentado a quem de direito, na forma, tempo e meio adequados, que permite conhecer uma avaliação ou fato, contribuindo para a tomada de decisões;

A informação subdivide-se em:

a) informações íntegras: Aquelas que apenas são alteradas através de ações autorizadas e planejadas;

b) informações integradas: Aquelas que fazem parte de um todo que se completam ou complementam.

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

XVII – Tecnologia da Informação: Conjunto de equipamentos e suportes lógicos, que visa coletar, processar, tratar, armazenar e distribuir dados e informações;

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

XIX – Integridade: Princípio de segurança que trata da salvaguarda da exatidão e confiabilidade da informação e dos métodos de processamento. Garantia de que as informações sejam exatas, que não sejam modificadas;

XX – Disponibilidade: Princípio de segurança que trata da garantia de que pessoas autorizadas obtenham acesso à informação e aos recursos correspondentes, sempre que necessário, ou seja, garantia que as informações estejam sempre disponíveis;

XXI – Segurança da Informação: É a preservação da confidencialidade, integridade, credibilidade e disponibilidade da informação; podendo, ainda envolver outros princípios, tais como autenticidade, responsabilidade, não repúdio e confiabilidade;

XXII – Credencial: 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 pelo servidor público municipal Técnico em Informática ou por empresas terceirizadas ou prestadoras de serviços, que tem a responsabilidade de dar suporte às ações do Sistema da Tecnologia da Informação;

XXIV – SPAM: 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.

CAPÍTULO IV BASE LEGAL

Art. 4º A presente Instrução Normativa tem como base legal a Constituição Federal, a Constituição Estadual, Lei Complementar nº 621/12 – Lei Orgânica do TCEES, Resolução TC nº 227/11, Lei Municipal nº 1.408/13 e Decreto Municipal nº 410/13 que regulamenta a sua aplicação e a Instrução Normativa SCI 01/13 – Norma das normas.

CAPÍTULO V RESPONSABILIDADES

Art. 5º São responsabilidades da Secretaria Municipal de Administração e Finanças como órgão central do Sistema Administrativo “STI” (Sistema de Tecnologia da Informação):

I – Promover a divulgação da Instrução Normativa mantendo-a atualizada e à disposição de todos os servidores, orientando as unidades executoras sobre a sua aplicação, e velando pelo seu fiel cumprimento;

II – Promover discussões técnicas com as unidades executoras e com a Unidade Central de Controle Interno para definir as rotinas de trabalho e os respectivos procedimentos de controle que devem ser objeto de alteração, atualização ou expansão sempre que se fizer necessário;

III – Promover o uso da informação e tecnologia da informação como instrumento estratégico de gestão e modernizador da Administração Pública Municipal.

Art. 6º São responsabilidades do Técnico de Informática:

I – Analisar periodicamente a efetividade da Política de Segurança da Informação, propondo mecanismos para sua melhoria contínua;

II – Avaliar as mudanças impactantes na exposição dos recursos de tecnologia da informação a riscos, identificando as principais ameaças;

III – Analisar criticamente os incidentes de segurança da informação e ações corretivas correlatas;

IV – Atender às solicitações da unidade responsável pela Instrução Normativa, quanto ao fornecimento de informações e à participação no processo de sua revisão;

V – Alertar à SEMAF sobre alterações que se fizerem necessárias nas rotinas de trabalho, objetivando sua otimização, tendo em vista, principalmente, o aprimoramento dos procedimentos de controle e o aumento da eficiência operacional;

VI – 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;

VII – Conscientizar os usuários internos em relação aos conceitos e as práticas de segurança da informação;

VIII – Comunicar ao superior imediato e à unidade competente em caso de comprometimento da segurança e quaisquer outras falhas, desvios ou violação das regras estabelecidas para adoção de medidas cabíveis;

IX – Prestar atendimento aos usuários, dando-lhes orientações, sanando dúvidas quanto aos recursos computacionais disponíveis, uso de *softwares*, internet e de como fazer uso desses recursos com racionalidade e o máximo de eficiência possível;

X – Cadastrar usuários nos sistemas disponíveis e de internet;

XI – Zelar pela segurança do servidor armazenador de dados, bem como pela guarda dos arquivos.

Art. 7º São responsabilidades da Unidade Central de Controle Interno:

I – Prestar apoio técnico por ocasião das atualizações desta Instrução em especial no que tange à identificação e avaliação dos pontos de controle e respectivos procedimentos de controle;

II – Avaliar, mediante atividade de auditoria interna, a eficácia dos procedimentos de controle inerentes a liberação e concessão de diárias propondo alterações na presente Instrução visando o aprimoramento dos controles.

CAPÍTULO VI DAS DISPOSIÇÕES INICIAIS

SEÇÃO ÚNICA Das obrigações e permissões dos usuários

Art. 8º A Política de Segurança da Informação 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. 9º A fim de resguardar a continuidade, integridade, credibilidade e disponibilidade das informações e serviços, devem ser adotados mecanismos de proteção.

Art. 10. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela Prefeitura de Itarana é considerada de sua propriedade e deve ser protegida, de acordo com esta Instrução Normativa.

Art. 11. 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. 12. Os sistemas e equipamentos utilizados para armazenamento de informações devem receber a mesma classificação dada à informação neles mantida.

Art. 13. Deverão ser realizadas auditorias periódicas dos ativos, de forma a aferir o correto cumprimento da Política de Segurança da Informação.

Art. 14. Fica assegurado ao Suporte Técnico, de ofício ou a requerimento do líder de unidade administrativa, necessariamente referendado pelo Secretário da pasta, a qualquer tempo, o poder de suspender temporariamente o acesso do usuário a recurso de tecnologia da informação da Prefeitura, quando evidenciados riscos à segurança da informação.

Art. 15. Caberá Técnico de Informática, conjuntamente com o Secretário de Administração e Finanças, 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. 16. 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 ISO/IEC 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. 17. Todos os recursos de tecnologia da informação da Prefeitura devem ser inventariados, classificados, atualizados periodicamente e mantidos em condição de uso.

Art. 18. Cada recurso de tecnologia da informação deverá ter um gestor formalmente designado.

Art. 19. Deverá ser implementado processo de gerenciamento de riscos, visando a identificação e a diminuição dos mesmos, associados às atividades críticas da Prefeitura.

Art. 20. 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. 21. 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.

CAPÍTULO VII DOS PROCEDIMENTOS

SEÇÃO I Das contas de acesso

Art. 22. Para utilizar os computadores e obter acesso ao correio eletrônico, internet da rede corporativa do Município, *software*, aplicativos e pastas em geral, o Secretário, o Chefe de Gabinete, o Procurador Geral ou o Controlador Interno, solicitará ao Técnico de Informática, a abertura de uma conta de acesso (*login*) e senha para o usuário que será credenciado e terá efetivada a sua permissão.

Art. 23. As contas de acesso aos recursos de Tecnologia de Informação terão a seguinte padronização:

I – E-mail Institucional: constará o nome do departamento seguido de @itarana.es.gov.br;

II – O e-mail institucional será utilizado pelo superior responsável do respectivo departamento, para fins de comunicação com outros órgãos e entidades, com o objetivo de centralizar as informações estratégicas da Secretaria em um único e-mail.

Parágrafo único. A forma de utilização dos e-mails institucionais seguirá rigorosamente esta Instrução Normativa.

Art. 24. O Técnico de Informática terá 30 (trinta) dias após a aprovação desta Instrução Normativa para solicitar a lista de todos os departamentos, setores, coordenadorias, etc, à Secretaria de Administração e Finanças, para que se efetue a padronização de todos os endereços de e-mail da Prefeitura.

Art. 25. No mês de fevereiro de cada ano o Técnico de Informática deverá atualizar e divulgar a todos os órgãos da Prefeitura e no sítio da Prefeitura, a lista dos e-mails institucionais.

Art. 26. 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. 27. Mudanças de lotação, atribuições, afastamento definitivo ou temporário do usuário deverá ser comunicado ao Técnico de Informática pelo Secretário da

respectiva pasta, para procedimentos de ajustes ou cancelamento de conta de acesso, cabendo a este Secretário a responsabilidade por qualquer uso indevido da credencial do usuário decorrente da não comunicação de algum dos eventos tratados neste item.

Parágrafo único. A comunicação deverá ser formalizada por ofício ou e-mail e ocorrer no prazo máximo de 24 (vinte e quatro) horas contadas da ocorrência de quaisquer situações elencadas no *caput* deste artigo.

Art. 28. 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. 29. 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. 30. 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.

SEÇÃO II

Dos programas e softwares

Art. 31. O usuário deverá informar imediatamente ao Suporte Técnico, sempre que o programa de antivírus enviar mensagem informando que algum arquivo está infectado.

Art. 32. 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, e-commerce, downloads, portais de entretenimento, dentre outros.

SEÇÃO III

Do ambiente de rede

Art. 33. O Técnico em Informática disponibilizará os pontos de rede necessários ao desenvolvimento das atividades dos órgãos da Prefeitura observado, contudo, os termos do contrato de prestação de serviço de internet. Qualquer alteração ou

criação de um ponto novo deverá ser precedida de comunicação ao Secretário de Administração e Finanças, ao Gestor do Contrato e ao Fiscal do Contrato.

Art. 34. É expressamente proibido o uso de meios ilícitos de acesso aos computadores, sistemas e arquivos do ambiente de rede computacional municipal.

Art. 35. É proibido o acesso remoto aos computadores da rede pública municipal sem o conhecimento ou consentimento do usuário.

Art. 36. É proibida a utilização de 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. 37. Fica proibido tentar burlar a utilização dos recursos computacionais do município com o objetivo de obter proveito pessoal ou violar sistemas de segurança estabelecidos.

SEÇÃO IV

Do correio eletrônico

Art. 38. O acesso ao sistema de correio eletrônico (e-mail) será disponibilizado aos usuários com necessidade manifesta de usá-lo como ferramenta de apoio às atividades profissionais.

Art. 39. É proibido participar, criar, ou distribuir voluntariamente mensagens indesejáveis, como circulares, manifestos políticos, correntes de cartas, SPAM ou similares que possam prejudicar o trabalho de terceiros, causar excessivo tráfego na rede ou sobrecarregar os sistemas computacionais desnecessariamente.

Art. 40. Não é permitido o uso de endereços de e-mail para troca de informações ligadas a práticas que infrinjam qualquer lei nacional ou internacional.

Art. 41. O usuário não deverá abrir e-mails com arquivos anexados quando não conhecer o remetente sob o risco de estar infectando com vírus seu equipamento.

SEÇÃO V

Das vedações no uso internet

Art. 42. Não é permitido ao usuário utilizar-se dos serviços internos de Internet do Município desvirtuando sua finalidade com o intuito de cometer fraudes.

Art. 43. 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 incentivo à violência ou outro material que possa violar qualquer lei aplicável.

Art. 44. Não é permitido desfrutar de quaisquer ferramentas para baixar músicas, vídeos ou jogos e outros, exceto se o acesso for necessário para realização das atividades do Setor.

Art. 45. É vedado o *download* de arquivos de qualquer natureza baseados na tecnologia Voip (Skype), exceto se o acesso for necessário para realização das atividades do Setor.

Art. 46. É proibida a utilização de ferramentas que burlem a segurança, para usufruir de serviços não autorizados.

Art. 47. É vedada a manutenção não autorizada de páginas pessoais ou de serviços particulares envolvendo comercialização pela internet utilizando os recursos computacionais do município.

SEÇÃO VI

Da assistência técnica aos recursos computacionais

Art. 48. Qualquer problema nos recursos computacionais da instituição deverá ser comunicado pelo usuário ao Suporte Técnico através do Chamado de Assistência Técnica em Informática, conforme o ANEXO II.

Parágrafo único. O envio do Chamado de Assistência Técnica em Informática será protocolado no Protocolo Geral da Prefeitura ou poderá ser através do e-mail informatica@itarana.es.gov.br, após o preenchimento, assinatura do mesmo pelo usuário interessado e sua digitalização em formato PDF.

Art. 49. O Técnico de Informática atenderá ao Chamado de Assistência Técnica em dias úteis até 24 (vinte e quatro) horas do comunicado apresentando solução no prazo de 72 horas, considerando dias úteis para o atendimento.

SEÇÃO VII

Do armazenamento de documentos e informações

Art. 50. O usuário deverá manter sigilo sobre os documentos e informações considerados estratégicos, confidenciais ou de interesse particular da administração pública municipal.

Art. 51. Os documentos e informações considerados estratégicos ou confidenciais deverão ser armazenados nos diretórios pessoais em pasta devidamente identificada por Secretaria.

Art. 52. 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 à luz da Lei Municipal de Acesso a Informação e seu Decreto regulamentador.

Art. 53. O usuário deve informar ao seu superior imediato quando informações ou aplicações consideradas estratégicas ou confidenciais forem encontradas sem o tratamento de segurança correto.

Art. 54. O diretório **C**: não deve ser utilizado pelo usuário para guardar documentos importantes ou confidenciais, sob o risco de perdê-los a qualquer tempo.

Art. 55. 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.

CAPÍTULO VIII

PROCEDIMENTOS PARA A REVOGAÇÃO DA INSTRUÇÃO NORMATIVA

Art. 56. Dos Procedimentos para revogar a Instrução Normativa:

I – Caso haja direito fundamentado na legislação pátria e interesse da Unidade de Controle Interno e/ou da Unidade Administrativa em revogar a Instrução Normativa, deve-se proceder da seguinte forma:

a) protocolar a solicitação devidamente justificada na Unidade Central de Controle Interno que, após análise, remeterá à Assessoria Jurídica para análise e emissão de parecer;

b) enviar ao Chefe do Poder Executivo ou para quem for delegado para rubrica e assinatura.

CAPÍTULO IX DAS DISPOSIÇÕES FINAIS

Art. 57. 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. 58. 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 de Informática.

Art. 59. Sempre que julgar necessário para a preservação da integridade dos recursos computacionais e a segurança da informação ou em caso de constatação e identificação de não conformidade às normas, o Técnico de Informática fará imediatamente o bloqueio temporário da conta de acesso e comunicará ao Secretário respectivo o teor da infração e o nome do responsável para que sejam tomadas as medidas cabíveis para a apuração dos fatos.

Art. 60. 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.

Art. 61. Todos os certificados de autenticidade, chaves de acesso, chaves seriais de *softwares*, mídias de instalação e demais documentos inerentes aos aspectos técnicos dos recursos de informática, devem ficar sob responsabilidade da Secretaria de Administração e Finanças, a qual disponibilizará às equipes de controladoria interna e externa, quando solicitadas.

Art. 62. 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. 63. Os termos contidos nesta Instrução Normativa, não eximem a observância das demais normas competentes, que devem ser respeitadas.

Art. 64. Caberá a SEMAF divulgar, cumprir e fazer cumprir as orientações contidas nesta Instrução Normativa e resolver, ouvida a Procuradoria e o Controle Interno, os casos omissos.

Art. 65. Esta Instrução Normativa deverá ser atualizada sempre que fatores organizacionais, legais ou técnicos assim o exigirem, a fim de verificar a sua adequação aos requisitos contidos na IN SCI Nº 01/13 – Norma das Normas, bem como manter o processo de melhoria contínua dos serviços públicos municipais.

Art. 66. Esta instrução entrará em vigor na data de sua publicação.

Itarana/ES, 17 de novembro de 2016.

ADEMAR SCHNEIDER
Prefeito do Município de Itarana

ROSELENE MONTEIRO ZANETTI
Secretária Municipal de Administração e Finanças

FLÁVIA COLOMBO DAL'COL
Controladora Interna em exercício

ROGÉRIO DELAI
Técnico de Informática



ANEXO I

TERMO DE RESPONSABILIDADE DE UTILIZAÇÃO DE ATIVOS E RECURSOS DE INFORMÁTICA DA PREFEITURA DE ITARANA

Secretaria:	Dpto/Setor:
Computador patrimônio n°:	
Monitor patrimônio n°:	
Servidor Responsável:	
Matrícula:	
E-mail institucional:	

Eu, _____ pelo presente instrumento, na condição de servidor(a)/colaborador(a) da Prefeitura de Itarana, comprometo-me a cumprir todas as orientações e determinações em função do vínculo jurídico e funcional que tenho com o Poder Executivo do Município de Itarana/ES, bem como com 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 e de acordo de que devo obedecer, cumprir e respeitar, as políticas, diretrizes, normas e procedimentos de Segurança da Informação da Prefeitura de Itarana, 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 manifestando o conhecimento de que o descumprimento dos compromissos por mim assumidos neste Termo sujeita-me às sanções aplicáveis.

Itarana/ES, ____ de _____ de _____.

Servidor Responsável

ANEXO II

CHAMADO DE ASSISTÊNCIA TÉCNICA EM INFORMÁTICA – ATI	
¹ Nº: ____/____/____	² Abertura do chamado: ____/____/____
³ Horário da Abertura: ____:____ horas	
⁴ Secretaria:	⁵ Dpto/Setor Requisitante:
⁶ Servidor Requisitante:	Matrícula:
⁷ Problema: (servidor requisitante relata o que está acontecendo com o equipamento)	
⁸ Manutenção/Causa: (o Técnico de Informática relata aqui o serviço realizado e o que pode ter causado o problema no equipamento)	
¹⁰ O chamado de ATI foi concluído dentro de 72 horas? () SIM () NÃO	
¹¹ Data da Solução: ____/____/____	
¹² Assinaturas:	
Técnico de Informática Matrícula:	Servidor Requisitante

Os campos 1, 2, 3 e 9 devem ser preenchidos pelo TI.

No campo 9 o TI (Técnico em Informática) deve relatar as observações em relação ao equipamento como forma de utilização, estado de conservação, local de trabalho, dentre outras verificações ocorridas durante o chamado. Prazos para o TI: O prazo de atendimento é de até 24 horas da abertura do chamado (campo 3) devendo a solução para o problema ocorrer até 72 horas após o atendimento.