INSTRUÇÃO NORMATIVA STI Nº 001

DISCIPLINA PROCEDIMENTOS DE SEGURANÇA FÍSICA E LÓGICA DOS EQUIPAMENTOS, SISTEMAS, DADOS E INFORMAÇÕES DA ADMINISTRAÇÃO DIRETA E INDIRETA.

Versão: 01

Data de Aprovação: 14 /jan. / 2014

Ato de Aprovação: Decreto nº 4.554 / 2014

Unidade Responsável: Setor de Tecnologia da Informação.

CAPÍTULO I

DA FINALIDADE

Art. 1º Dispor sobre as normas gerais e procedimentos de segurança física e lógica dos equipamentos, sistemas, dados e informações da Administração Direta e Indireta do Município de Conceição da Barra, Estado do Espírito Santo.

CAPÍTULO II

DA ABRANGÊNCIA

Art. 2º Abrange o Setor de Tecnologia da Informação enquanto unidade responsável e todas as unidades da estrutura organizacional da Administração Direta e Indireta do Município de Conceição da Barra, Estado do Espírito Santo como unidades executoras, em especial.

CAPÍTULO III

DOS CONCEITOS

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

I– Informação: todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

II– Tecnologia da Informação - TI: área de conhecimento responsável por criar,administrar e manter a gestão da informação através de dispositivos e equipamentos para acesso, operação e armazenamento dos dados, de forma a gerar informações para tomada de decisão.

III–Segurança da Informação: está relacionada com a proteção de um conjunto dedados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade das Informações supostas.

IV – Segurança Física: é a segurança em nível das infraestruturas materiais que abrange todo o ambiente onde os sistemas de informação estão instalados.

a) Ameaças Físicas: Incêndios, desabamentos, relâmpagos, alagamentos, acesso indevido de pessoas, forma inadequada de tratamento e manuseio do Material;

b) Mecanismos de Segurança Física: Portas, trancas, paredes, revestimento em equipamento, blindagem, guardas, extintores, saída de emergência; etc;

d) Controle de Acesso: são recursos e autorizações e as suas restrições de acessos aos ativos de informações e acesso à internet.

V– Segurança Lógica: forma como um sistema é protegido no nível de sistema operacional e de aplicação. Normalmente é considerada como proteção contra ataques, mas também significa proteção de sistemas contra erros não intencionais, como remoção acidental de importantes arquivos de sistema ou aplicação.

a)Ameaças Lógicas: vírus acessos remotos à rede, backups desatualizados,violação de senhas, etc.

b) Mecanismos de segurança Lógica: detectores de intrusões, anti-vírus, firewalls,firewalls locais, filtro anti-spam, fuzzers, analisadores de código, etc.

c) Ameaças a Perda da Confidencialidade: quando houver a perda ou quebra do sigilo de uma determinada informação sendo por sua vez senha, logins, e acessos remotos;

d) Ameaças a Perda da Integridade: sendo quando a exposição de uma determinada informação por alguma pessoa ou individuo não autorizado perante os setores;

e) Ameaças a Perda de Disponibilidade: este acontece quando a informação deixa de estar acessível por quem necessita dela.

VI – Backup: é a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou dados corrompidos ou equipamentos danificados;

VII – Usuário: pessoa física cadastrada em um ou mais sistemas informatizados para acesso a informações;

VIII – Cadastro: procedimento de criação de usuário (Login/ID) para acesso aos sistemas informatizados;

IX – 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;

X – *Enterprise Resource Planning - ERP*: são sistemas de informação que integram todos os dados e processos de uma organização em um único sistema;

XI – *Internet Protocol – IP*: ou seja, Protocolo de Internet que corresponde ao padrão de endereçamento, por meio do qual um computador é identificado na Internet por um número exclusivo. Baseia-se em um conjunto de 32 bits que atribui um endereço ao computador, afim de indetifica-lo na Internet. Desempenha funções como rastrear endereços dos nós, caminho para envio de mensagens, reconhecimento de mensagens recebidas;

XII – ***Virtual PrivateNetwork –*** VPN**:** ou seja,Rede Privativa Virtual, que se utiliza da infraestrutura de uma rede pública de telecomunicações, como a Internet, por

exemplo, para a transmissão de informações confidenciais. Os dados transmitidos são encriptados. Sua implementação se dá por meio de firewalls instaladas entre as redes particulares e a Internet, formando túneis virtuais, pelos quais trafegam as informações, protegendo-as do acesso de usuários não autorizados;

XIII – *MAC – ADDRESS*:corresponde a Endereço MAC, ou seja, endereço de Media *Access Control* que consiste no endereço associado com cada dispositivo de hardware na rede.

CAPÍTULO IV

DA BASE LEGAL

Art. 4º A presente Instrução Normativa integra o conjunto de ações, de responsabilidade do Chefe do Poder Executivo, no sentido de atendimento aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência, dispostos no art. 37 da Constituição Federal, amparado nos artigos 31, 70 e 74 da Constituição Federal, Lei Nº.12.737, de 30 de novembro de 2012 que Dispõe sobre a tipificação criminal de delitos informáticos e Normas Internacionais de Segurança da Informação, bem como Legislação Municipal que dispõe sobre o Estatuto dos Servidores Públicos – Lei Municipal nº 2.052/99, Lei Complementar Municipal nº 27/2011 que institui o Sistema de Controle Interno Municipal e Instrução Normativa SCI nº 001/2012.

CAPÍTULO V

DAS RESPONSABILIDADES

Art. 5º Compete ao **Setor de Tecnologia da Informação:**

I – promover a divulgação e a implantação desta Instrução Normativa, mantendo-a atualizada;

II – efetuar o acompanhamento sobre a efetiva observância das instruções normativas as quais o Sistema de Segurança da Informação está sujeito;

III – promover discussões técnicas com o setor de Tecnologia da Informação, visando aprimoramento das instruções normativas;

IV – manter a Instrução Normativa à disposição de todos os servidores relacionados ao setor de TI – Tecnologia da Informação;

V – gerenciar identidade e controle de acesso lógico;

VI – controlar o acesso Físico;

VII – controlar o acesso à internet, através de monitoramentos;

VIII – verificar formas de utilização do e-mail, enviar, receber e baixar;

IX – configurar e instalar o sistema operacional e demais softwares em todos os computadores portáteis e estações de trabalho;

X – orientar sobre as formas de utilização dos equipamentos de Tecnologia da Informação;

XI – orientar sobre utilização de programas e aplicativos;

XII – zelar pelo armazenamento das informações geradas;

XIII – gerenciar as contingências e garantir a continuidade do processo de trabalho da rede, tanto no tocante a estrutura de software como de hardware, mantendo equipe a disposição para atendimento às demandas em tempo adequado assegurando a não paralisação dos serviços públicos;

XIV – coordenar as ações necessárias na ocorrência de incidentes de segurança e do meio físico;

XV – coordenar ações em determinadas ocorrências de acidentes com hardware e lógico;

XVI – recepcionar e conferir a documentação necessária ao cadastro, suspensão e exclusão de usuários, à habilitação e inabilitação de módulos e ao fornecimento de senhas;

XVII – utilização de *lacre de segurança* em todos os equipamentos de hardwares pertencentes à administração direta ou indireta, os quais deverão ser ordenados sistematicamente com número de série único, com identificação do órgão, independente do modelo, o qual devera ser gerenciado e controlado pelo Setor de Tecnologia da Informação, (de acordo com critérios e regramentos definidos em

norma específica.) que produzirá relatório mensal dos procedimentos o qual deverá ser enviado ao setor de patrimônio para acompanhamento sistêmico das ocorrências, tanto por ocasião da colocação do lacre quanto em casos de ruptura para manutenção do equipamento ou qualquer outro fim. Cabendo ao setor de patrimônio fazer constar no *registro* de controle do equipamento o numero do respectivo *lacre de segurança;*

XVIII – projetar, administrar e supervisionar as redes de computadores;

XIX – desenvolver ou contratar e implantar sistemas de informação voltados às atividades da administração pública como um todo;

XX – propor a adoção de normas técnicas e procedimentos relativos à manutenção, instalação e configuração de software e hardware;

XXI – gerir os sistemas de informação próprios ou de terceiros e demais recursos de informática, bem como relativo à transmissão de dados;

XXII – estabelecer mecanismos de permissão de acesso a partir de pontos externos e internos;

XXIII – desenvolver e aplicar normas técnicas e procedimentos relativos aos recursos de informática;

XXIV – estabelecer uma política de treinamento para os servidores municipais, de modo a aperfeiçoar a relação deste para com o equipamento, softwares específicos (automação e produtividade) e outras ferramentas que o auxiliem na otimização das atividades de sua competência;

XXV – promover a guarda da mídia de software pertencente à administração;

XXVI – manter organizada e atualizada a biblioteca de mídia de softwares (quaisquer produtos), sendo de competência única e exclusiva do Setor de Tecnologia da Informação a instalação de softwares nos equipamentos ou a quem este delegar, não sendo admitida a instalação de softwares que não sejam originais e legalmente adquiridos, defendendo assim os direitos autorais (copyright) e demais leis reguladoras do uso e licença de softwares;

XXVII – desenvolver a política de segurança propondo seu emprego para a administração municipal direta e indireta, utilizando sistemas de segurança, ou controles ou quaisquer outros mecanismos que julgar adequado, bem como poderá realizar, quando julgar necessário, a avaliação periodicamente do uso dos recursos de informática e redes;

XXVIII – estabelecer e regulamentar a política de segurança e de acesso às informações, por quaisquer das vias conhecidas seja por Internet, Intranet ou outro modelo, criando regras e procedimentos de utilização;

XXIX – manter no Setor de Tecnologia da Informação, informações cadastrais, com os dados de todos os usuários autorizados;

XXX – controlar o acesso físico aos equipamentos sob a responsabilidade STI;

XXXI – cadastrar e manter atualizada as contas e/ou e-mail de todos os usuários autorizados;

XXXII – não permitir que softwares licenciados para uso da administração direta ou indireta sejam copiados por terceiros ou instalado em computador não autorizado, ficando igualmente vedado a qualquer usuário ou administrador usar softwares não licenciados pela PMCB;

XXXIII – rever os acessos de usuários que deixarem de ser membros da comunidade de servidores da administração direta ou indireta ou que assumirem novas funções, tão logo venha receber comunicado que deverá ser providenciado imediatamente pelo Setor de Recursos Humanos – SRH, assim que se fizer ciência do fato, devendo, ainda, gerar mensalmente Relatório Mensal que também será encaminhado formalmente ao Setor de TI;

XXXIV – manter, no Setor de Tecnologia da Informação, um registro das ocorrências de violação do regulamento;

XXXV – buscar a padronização dos softwares (produtividade, navegador, correio eletrônico, antivírus e outras, mantendo-os continuamente atualizados), bem como fornecer orientação sobre o uso correto destes recursos;

XXXVI – estabelecer, com atualização constante, os requisitos mínimos dos equipamentos de informática a serem adquiridos por qualquer meio de processo licitatório, orientando ainda a Seção de Compras na qualificação destes equipamentos;

XXXVII – desenvolver mecanismos com a finalidade de elaborar, em periodicidade a ser definida, cópias de segurança (*backup's*) de todos os dados das atividades desenvolvidas pela Administração Municipal, nos servidores corporativos da administração direta e indireta;

XXXVIII – implantar e manter disponível a infraestrutura de sistemas, equipamentos e segurança dos serviços de Internet, Intranet e Correio Eletrônico;

XXXIX – monitorar o padrão de utilização dos serviços de Internet, Intranet e Correio Eletrônico identificando condutas inapropriadas;

XL – compete exclusivamente ao Setor de Tecnologia da Informação a realização de auditorias internas nos equipamentos, ou a pessoa por este indicada e por ele capacitada para este fim;

XLI – as senhas de servidores físicos, virtuais, vm ware, firewall – pf senser, ativos de rede, tais como switch, roteadores, senhas máster de softwares de gestão locados ou desenvolvidos pelo próprio setor de TI, ficarão sob a guarda exclusiva do Gerente de Tecnologia da Informação e do Secretário da pasta a que o órgão central de TI esteja diretamente vinculado, credenciado com idêntico status de acesso;

XLII – compete exclusivamente ao Setor de Tecnologia da Informação a definição, guarda e instalação de todos os equipamentos tipo servidores de rede e demais equipamentos para o perfeito funcionamento da rede informatizada no âmbito da administração direta e indireta, garantindo assim a centralização em seu Data Center, cumprindo desta forma todos os termos desta Instrução Normativa.

Art. 6º Compete aos **Usuários** das ferramentas de tecnologia da informação:

I – assinar Termo de Responsabilidade (Anexo II), formalizando a ciência e o aceite da Normativa, bem como estar ciente sobre a responsabilidade do seu cumprimento;

II – comunicar imediatamente a área de Tecnologia da Informação – T.I. qualquer descumprimento ou violação desta Normativa e seus procedimentos;

III – zelar pela ordem das instalações do local e do equipamento disposto.

IV – buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;

V – não manusear alimentos e bebidas próximo aos equipamentos de Informática;

VI – assumir atitude pró-ativa no que diz respeito à proteção das informações da entidade;

VII – assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades de trabalho de cada setor e ao interesse deste órgão.

VIII – comunicar ao setor de TI qualquer ocorrência que comprometa o bom funcionamento do equipamento de hardware ou de rede, abstendo-se sempre de proceder qualquer operação que comprometa os resultados, de tal ordem que surgindo qualquer necessidade de intervenção ou manutenção a equipe técnica deve ser informada do fato e motivo que possa ter ensejado o ocorrido;

IX – proteger do acesso de terceiros, sua identificação na rede corporativa (*login)* através de senhas secretas e procedimentos de segurança, sendo de sua inteira responsabilidade o uso de sua conta de acesso à rede e outros tipos de autorização, que são de uso individual e intransferível, não podendo ser compartilhados com terceiros, salvo em situações especiais que a unidade administrativa julgar necessária, por prazos curtos e pré-determinados, o que se fará, somente mediante autorização do Secretário da pasta ou autoridade competente decorrente de inquérito administrativo;

X – a total responsabilidade pela manutenção de senhas de segurança, devendo seguir normas e procedimentos padronizados e divulgados através de normas internas de procedimentos editadas no âmbito do Sistema de Tecnologia da Informação;

XI – reconhecer e honrar a propriedade intelectual e os direitos autorais, sob pena de ser imputado a este os ônus relativos ao uso inadequado dos softwares de terceiros;

XII – a ocorrência de ações indevidas que venham a ser efetuadas a partir de sua conta de acesso à rede;

§1º. É vedado ao usuário:

I – facilitar o acesso de usuários não autorizados, aos recursos de informática e redes da administração direta ou indireta, executando, instalando ou modificando a configuração de software ou hardware;

II – invadir a privacidade dos de mais usuários da rede ou de terceiros;

III – conectar computadores mono e/ou multiusuário e servidores de rede ou similares de qualquer espécie, à rede de computadores da administração direta e indireta, sem notificação e autorização dos administradores ou dos supervisores responsáveis pela rede computacional, assim como acessar a internet por outro provedor que não seja a do respectivo órgão/instituição;

IV – sobrecarregar os recursos computacionais ou de rede corporativa;

V – violar o *lacre de segurança* fixado no equipamento ou permitir que terceiro o faça.

§2º. Nenhum membro da comunidade de usuários pode, sob quaisquer circunstancias, usar computadores e redes da administração direta ou indireta para difamar, caluniar ou molestar outras pessoas.

§3º. Para os fins do disposto no parágrafo anterior, entende-se por molestamento o uso intencional dos recursos de informática ou redes para:

I – perturbar, amedrontar, ameaçar ou ofender pessoas usando linguagem ou qualquer outro mecanismo ou material que comprometam a integridade física ou moral do receptor ou de sua família;

II – contatar alguém várias vezes com a intenção de perturbá-la, enviando ou não mensagens, seja quando não existe uma proposta de comunicação ou quando o receptor expressa o desejo de finalizar a comunicação;

III – indisponibilizar recursos computacionais de forma intencional.

Art. 7º Compete a **Unidade de Central de Controle Interno – UCCI**:

I – prestar apoio técnico por ocasião da Instrução Normativa, 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 o cumprimento e a eficácia dos procedimentos de controle desta Instrução Normativa, para aprimoramento das atividades de gestão.

CAPÍTULO VI

DOS PROCEDIMENTOS

SEÇÃO I

DO ACESSO ÀS INFORMAÇÕES

Art. 8º O acesso especial a senhas, informações ou outros privilégios só podem ser usados para o exercício de tarefas oficiais, como supervisão e administração das redes, acesso que somente poderá ser delegado, exclusivamente a profissional que tenha vinculo com a Administração, e formação devidamente comprovada na área de gestão de rede, por delegação em ato específico da autoridade competente, no qual o agente assumirá de forma expressa, a responsabilidade pelos resultados que decorram de operações por meio de sua senha de acesso.

Art. 9º Informações obtidas por meio de direitos especiais e privilégios devem ser tratados como privativas e totalmente confidencias pelos administradores de redes, que responderão por qualquer uso indevido.

Art. 10 Ao deixar de pertencer ao quadro de servidor público da administração direta ou indireta, ou ao ser nomeado para assumir uma nova função, atividade ou responsabilidades, o usuário não poderá fazer uso de benefícios, contas, senhas de acesso, direitos especiais ou informações aos quais não está em razão da função, autorizado em sua nova situação, de tal ordem que os privilégios especiais não são incorporados permanentemente aos direitos dos usuários.

Art. 11 Os órgãos centrais de Tecnologia da Informação poderá suspender todos os privilégios de usuário em relação ao uso das redes e computadores sob sua responsabilidade, por razões disciplinares ou relacionadas à segurança dos dados e informações e ao bem-estar dos servidores da administração direta ou indireta, respectivamente.

Art. 12 É facultado aos administradores de rede o acesso a todos os equipamentos ligados a rede, de forma a ser possível à realização de procedimentos de auditoria, controle, manutenção e segurança que se fizerem necessários, na forma desta Instrução Normativa.

Parágrafo único – Na hipótese em que o processo de intervenção do setor de TI possa incorrer em lentidão ou mesmo interrupção do sistema, o fato deverá ser comunicado previamente por meio de comunicação eletrônica (e-mail) com antecedência mínima de três (03) dias a todos os Secretários, Procurador e Controlador, ficando estes incumbidos de preparar a equipe para a ocorrência, de tal ordem que não cause prejuízo aos trabalhos.

SEÇÃO II

DO CADASTRO E ACESSO DOS USUÁRIOS

Art. 13 O cadastro e acesso dos usuários às ferramentas de Tecnologia da Informação se darão mediante solicitação de habilitação ou inabilitação de usuários aos sistemas informatizados que serão processados, exclusivamente, pelo órgão gestor do Sistema de Tecnologia da Informação, atendidas as condições estabelecidas a seguir:

I – o pedido de cadastro dos usuários, bem como alteração, exclusão, bloqueio e desbloqueio, será realizado através do preenchimento do formulário “Controle de Acesso aos Sistemas” (Anexo I), o qual deve ser devidamente preenchido e assinado pelo servidor (a) e devidamente ratificado pelo Secretário Municipal ao qual esteja o servidor a ele subordinado;

II – o acesso do usuário aos sistemas informatizados é feito mediante uso de senha pessoal e intransferível e sua autorização de uso não implica direito de acesso imotivado aos sistemas e informações;

III – o formulário "Controle de Acesso aos Sistemas" (Anexo I), será emitido em 2(duas) vias, sendo uma via arquivada no setor de Tecnologia da Informação e outra para arquivo do órgão solicitante;

IV – a habilitação de usuário para operar os sistemas operacionais, se dará somente após demonstrar-se apito, na avaliação do agente do setor de TI responsável pelo treinamento. Caso contrário poderá o agente responsável pelo treinamento e avaliação, recusar o cadastro do pretenso usuário, mediante justificativa formal endereçada ao superir imediato do pretenso usuário;

SEÇÃO III

DA REALIZAÇÃO DE BACKUP

Art.14 A execução dos backups e respectiva verificação são de responsabilidade da área de Tecnologia da Informação e se fará na forma deste artigo:

I – os Backups do banco de dados dos sistemas administrativos (Sistemas de Contabilidade, Compras, Licitação, Almoxarifado, Patrimônio, Recursos Humanos, entre outros) serão executados de forma automatizada, pelo Setor de Tecnologia da Informação;

II – os Backups de estações de trabalho e computadores portáteis serão realizados sempre que houver necessidade de manutenção e/ou conserto dos equipamentos ou por outras circunstâncias que representem alguma ameaça ou risco à base dedados;

III – cópia fiel das informações será armazenada em unidade externa, em CD/DVD ou HD externo, em outra máquina da rede ou em pen-drive;

IV – a responsabilidade pela segurança e integridade dos backups é da área de Tecnologia da Informação;

V – preferencialmente, as cópias e geração dos Backups serão realizadas utilizando software livre, ou quando for o caso, manualmente através do recurso CTRL + C do hardware.

VI – é vedada a realização backup de arquivos e softwares que não estão sob a licença de uso da Prefeitura Municipal de Conceição da Barra.

SEÇÃO IV

DA POLÍTICA DE LOGIN / SENHAS / UTILIZAÇÃO

Art. 15 A política de logins, senhas e utilização da estrutura de Tecnologia da Informação se dará atendendo as seguintes diretrizes:

I – a criação do login e senha aos usuários serão processadas nos termos do art. 13desta Instrução Normativa, pela área de T.I;

II – a senha deverá conter, no mínimo, 6 (seis) caracteres alfanuméricos, ou seja,composta por letras e números;

III – recomenda-se que as senhas sejam alteradas, no mínimo, uma vez por ano e sempre que o usuário perceber que a mesma pode ser de conhecimento de outrem;

IV – em face do seu caráter de pessoalidade, a senha é intransferível, não podendo ser compartilhada, divulgada a outra pessoa, anotada em papel ou em sistema visível, ou de acesso não protegido;

V – é vedado credenciar ao uso da(s) senha(s) indicada(s) no inciso XLI do art. 5º desta IN, agente que não comprove qualificação compatível e que não possua vinculo efetivo direto com o setor de TI da administração direta ou indireta. O agente que descumprir ou permitir que se descumpra o dispositivo em questão responderá civil e criminalmente pela prática do ato, arcando pessoalmente com todas as suas consequências.

VI – para segurança e o livre acesso a informação e banco de dados, necessária execução de seu ofício, atendidas as limitações expressas no ato de credenciamento na forma desta IN, o servidor público manterá um cadastro pessoal de seu nome login/usuário e senha de acesso aos computadores, site, preservando ao Poder Executivo o direito de acesso ao banco de dados para continuidade do serviço público ou em caso de auditoria por parte da Unidade Central de Controle Interno;

VII – os equipamentos que pertencem a Administração Municipal ficam resguardados o direito monitorar e cadastrar os usuários e senhas;

VIII – o tempo máximo de inatividade de uma conta é de 04 (quatro) meses. Para reabertura da conta após esse período, o usuário deverá enviar solicitação ao Setor de Tecnologia da Informação;

IX – as contas inativas serão excluídas anualmente ou quando se fizer necessário, nas hipóteses definidas nesta Instrução Normativa;

SEÇÃO V

DAS CONFIGURAÇÕES DE REDE

Art. 16 As configurações de rede é ato privativo do Setor de Tecnologia da Informação, sendo estabelecidas as seguintes limitações:

I – é proibido aos usuários realizar alterações nas configurações de rede e de inicialização das máquinas, sendo estas atribuições exclusivas do setor de T.I;

II – não é permitido fazer download e/ou instalar software de gerenciamento de download para efetuar baixas de músicas e filmes sem autorização expressa e formal do Setor de Tecnologia da Informação, desde que seja de interesse público;

III – é proibido aos funcionários utilizarem equipamentos e os serviços de internet para acesso on-line a outros bancos de dados ou sistema que não seja utilizado pela Prefeitura Municipal.

SEÇÃO VI

DA UTILIZAÇÃO DE EQUIPAMENTOS DE INFORMATICA PARTICULARES

Art. 17 Fica proibido no ambiente público alcançado pelos efeitos desta Instrução Normativa:

I – à entrada de equipamentos (computador/notebook/netbook) de particulares ou de uso próprio qualquer agente;

II – o uso de equipamentos de rede que não pertença aos órgãos da administração direta ou indireta;

III – a conexão ou acesso a informação da administração direta ou indireta;

IV – conserto ou reparação pelo Setor de Tecnologia da Informação de equipamentos que não pertençam ao órgão da administração direta ou indireta.

Parágrafo único – Somente poderá ser permitida a utilização dos equipamentos evidenciados no neste artigo, a agente de instituições públicas de controle externo (INSS, Tribunais de Contas, CREA, Ministério do Trabalho, etc) quando em missão institucional, e, empresas de suporte técnico contratadas pelo Município, desde que previamente informado, oficialmente, ao Setor de Tecnologia da Informação que se incumbirá de promover o suporte necessário, com as cautelas que assegurem a integridade do acervo de informações municipais, na forma desta Instrução Normativa.

SEÇÃO VII

DA SEGURANÇA E ACESSO AOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

Art. 18 A segurança e acesso aos recursos de tecnologia da informação se dá na forma deste artigo:

I – o acesso aos ativos centrais da entidade e ao ambiente informatizado, rack, servidores, central telefônica, firewall e sala de manutenção, deve ser motivado por necessidade de serviço, devendo ser controlado e restrito às pessoas autorizadas;

II – a utilização dos recursos de tecnologia da informação será monitorada, com a finalidade de detectar divergência entre as normas que integram a Política de Segurança da Informação e os registros de eventos monitorados, fornecendo evidências nos casos incidentes de segurança;

III – as permissões de acesso devem ser graduadas de acordo com as atribuições, renovadas periodicamente conforme instrução específica que receberão dá área técnica;

IV – os novos usuários deverão ser orientados quanto às normas e procedimentos de acesso e utilização dos recursos de Tecnologia da Informação;

V – arquivos de origem desconhecida nunca devem ser abertos, muito menos executados.

SEÇÃO VIII

DO ACESSO E USO DA INTERNET

Art. 19 O acesso e uso da Internet ficam condicionados às seguintes permissões e limitações:

I – não são permitidas conexões por meio de placas, equipamentos de fax-modem,

ou outras tecnologias móveis;

II – a Administração Municipal poderá monitorar os acessos às páginas da Internet com o intuito de identificar, bloquear e notificar formalmente os usuários internos ou colaboradores sobre as páginas com conteúdo impróprio para o ambiente de trabalho e casos detectados de queda de produtividade em função do uso abusivo desta ferramenta;

III – não são autorizados acessos a páginas de conteúdo impróprio ao ambiente de trabalho, como por exemplo: pornografia, downloads, youtube, vídeos, jogos,músicas entre outros;

V – o Setor de Tecnologia da Informação deverá manter arquivo do monitoramento do uso da Internet e encaminhar as situações que estiverem em desacordo com a presente Instrução Normativa ao superior imediato do agente que tenha transgredido a norma com cópia a Controladoria Geral Municipal.

SEÇÃO IX

DO ACESSO REMOTO EXTERNO E INTERNO

Art. 20 O acesso remoto à rede de computadores da Prefeitura Municipal de Conceição da Barra pelo setor de Tecnologia da Informação passará pelos seguintes procedimentos:

I – o acesso remoto aos computadores e notebooks dos agentes públicos dependerá sempre da prévia autorização por parte do usuário no momento em que se der atendido pelo profissional do setor de TI;

II – para que o agente do setor de TI efetue o acesso de que trata o inciso I, precederá da confirmação da intervenção pelo solicitante que se dará com o acionamento do dispositivo de "aceite" que será projetada na tela do equipamento, por meio do software de conexão remota através do sistema operacional instalado em cada equipamento ou software legalmente licenciado pelo órgão da

administração direta ou indireta;

III – o acesso via VPN (Vitual Private Network) ou Área de Trabalho Remota, pelos usuário internos, parceiros e agentes públicos da administração direta ou indireta do município dar-se-á mediante adesão expressa ao Termo de Responsabilidade de Acesso Remoto à rede corporativa do órgão da administração direta ou indireta, nos termos do Anexo IV desta Instrução Normativa.

SEÇÃO X

DO RECADASTRAMENTO

Art. 21 Todos os acessos criados para os sistemas e equipamentos da Administração Municipal até a data da publicação desta Instrução Normativa terão um prazo de 60 (sessenta) dias para serem recadastrados.

Art. 22 O recadastramento de usuários para acesso a equipamentos e sistemas no âmbito da Administração direta e indireta fica condicionada à solicitação do usuário, ratificada pelo Secretário Municipal da pasta a quem o servidor esteja a ele subordinado.

Art. 23 O processo de recadastramento obedecerá aos procedimentos estabelecidos neste instrumento e a solicitação do recadastramento ficará a cargo do titular da secretaria/órgão ao qual o usuário está lotado.

Art. 24 Vencido o prazo, o acesso deverá ser cancelado pelo Setor de Tecnologia da Informação.

CAPÍTULO VII

DA CLASSIFICAÇÃO DAS INFRAÇÕES

Art. 25 É considerada infração grave, para fins desta Instrução Normativa:

I – criar ou propagar vírus, de qualquer natureza, de forma intencional, ou arquivos do tipo “Cavalo de Tróia”;

II – danificar serviços e arquivos;

III – destruir ou estragar intencionalmente equipamentos, software ou dados pertencentes à administração direta ou indireta, a outros usuários;

IV – obter acesso a qualquer recurso que não lhe tenha sido devidamente autorizado, na forma desta Instrução Normativa;

V – destruir e/ou instituir direitos para outros usuários;

VI – instalação de software não autorizado pelo STI.

Art. 26 É considerado conteúdo inapropriado para acesso, através da infraestrutura de informática da administração direta ou indireta, qualquer página, e-mail ou arquivo que contenha referências a:

I – nudez total ou parcial;

II – atos sexuais;

III – pornografias;

IV – erotismos;

V – terminologia de baixo calão;

VI – violência;

VII – racismo;

VIII – satanismo e ocultismo;

IX – intolerância;

X – extremismo;

XI – material ilegal ou dados que levem a condutas ilegais;

XII – cassinos e jogos;

XIII – sites de *hacker's*;

XIV – salas públicas de conversação on-line *(chat)*;

XV – serviços de intermediação de navegação *(anonimizer)*.

CAPÍTULO VIII

DOS PROCEDIMENTOS E DAS SANÇÕES

Art. 27 Os interessados, ao se cadastrarem como usuários dos recursos de informática e redes da administração direta ou indireta, deem preencher e assinar

uma ficha cadastral, manifestando conhecimento e concordância com as normas específicas e padrões para utilização e acesso aos recursos de cada unidade administrativa.

Art. 28 A ficha cadastral deverá ser mantida sob o controle do Setor de Tecnologia da Informação em caráter confidencial e as informações nela constantes não poderão ser utilizadas para qualquer finalidade não relacionada ao controle, a segurança e a integridade dos sistemas.

Art. 29 Os usuários, supervisores e administradores de rede têm o dever de denunciar qualquer desrespeito a este regulamento, tomando imediatamente as seguintes providencias:

I – comunicar ao superior imediato, à direção da unidade administratva e ao Setor de Tecnologia da Informação;

II – manter o sigilo, para garantir a segurança e a conservação dos recursos.

SEÇÃO I

DAS INCIDENCIAS E CONSEQUENCIAS

Art. 30 O primeiro incidente envolvendo um usuário, sendo este considerado de proporções leves, na forma desta Instrução Normativa, será tratado pelo Setor de Tecnologia da Informação por meio de alerta formal ao usuário pelo STI, com registro da ocorrência que será ordenada em sequencia cronológica de numero e data a ser mantida no acervo de controle do STI.

Art. 31 No caso de reincidência e incidentes considerados graves deverá o STI proceder ao registro da ocorrência, informando o caso ao superior imediato do agente e aos órgãos competentes, para determinação das medidas administrativas e/ou repressivas a serem impostas.

SEÇÃO II

DAS PENALIDADES

Art. 32 O descumprimento as regras definidas nesta Instrução Normativa serão punidas na forma deste artigo, não obstante as demais sanções aplicáveis a cada

caso, levando em conta o conjunto de normas que orientam a relação do agente com a estrutura pública de gestão.

I – pena leve: advertência escrita à pessoa do usuário infrator, instruída com cópia ao superior imediato;

II – pena grave: aplicáveis nos casos de reincidência e/ou constatação de infração grave, serão punidas na forma desta Instrução Normativa, e neste caso será instaurado pelo STI procedimento administrativo formal,devidamente protocolado, contendo relatório circunstanciado dos fatos e reunião de todos os elementos de prova que a tenha fundamentado, endereçando-se à Comissão Administrativo Disciplinar, por intermédio do órgão de administração geral de recursos humanos.

Parágrafo único – as demais hipóteses de violação às normas afetas ao STI, poderão ser punidas com suspensão temporária ou permanente de privilégios de acesso aos recursos computacionais, após avaliação da gravidade da infração.

CAPÍTULO IX

DAS CONSIDERAÇÕES FINAIS

Art. 33 Os Procedimentos contidos nesta Instrução Normativa não eximem a observância das demais normas aplicáveis ao assunto.

Art. 34 A inobservância das diretrizes estabelecidas nesta Instrução Normativa constitui ato de insubordinação, omissão de dever funcional e será punida na forma prevista em lei.

Art. 35 O descumprimento do previsto nos procedimentos aqui definidos será passível de instauração de Processo Administrativo para apuração de responsabilidade.

Art. 36 Os esclarecimentos adicionais a respeito deste documento poderão ser obtidos junto à controladoria e/ou Setor de Tecnologia da Informação.

Art. 37 Toda estrutura administrativa, seja a Administração Direta e Indireta, ou ainda as que venham a ser criadas, deverão observar as disposições do presente regulamento, sob pena de incorrer nas penalidades previstas.

Sede Administrativa da Prefeitura Municipal de Conceição da Barra, Sala da Controladoria Geral Municipal, aos quatorze dias do mês de janeiro do ano de dois mil e quatorze.

Ronald Joseph Edmond Maliniak
Gerente – Setor de Tecnologia da Informação
Matricula nº 5923

Judson Conceição Azevedo
Gerente – Setor de Tecnologia da Informação
Matricula nº 10923

Vanei Rodrigues Passos
Analista de Sistemas
Matricula nº 9772

Mervaldo de Oliveira Faria
Subsecretário de Tributação e Informática
Matricula nº 700358

Francisco Bernhard Vervloet
Secretário Municipal de Administração
Matricula nº 9848

Claudia Regina Vieira da Cunha
Controladora Geral Municipal
Matricula nº 402

Homologado na forma definida no art. 13, IX da IN- SCI nº 001/2012, através do Decreto nº 4.540, de 06 de dezembro de 2013.

Jorge Duffles Andrade Donati
Prefeito

ANEXO I – IN STI Nº 001

CONTROLE DE ACESSO AO SISTEMA DE INFORMATICA E INTERNET
AGENTE INTERNO

SITUAÇÃO

1 – IDENTIFICAÇÃO DO SOLICITANTE	
ÓRGÃO/SETOR:	MATRICULA:
TELEFONE:	EMAIL:
SUPERIOR IMEDIATO DO SERVIDOR:	
ATIVIDADES EXECUTADAS INTERNET/SERVIDOR:	

2 – IDENTIFICAÇÃO DO SERVIDOR (A)	
NOME:	CPF:
CARGO:	VINCULO:

SOLICITA HABILIDTAÇÃO DO SERVIDOR IDENTIFICADO NOS SEGUINTES MÓDULOS / SISTEMAS		
SISTEMA/INTERNET (software/site)	MODULOS/ACESSO	
		USO DIÁRIO ( ) SIM ( ) NÃO

NÍVEL DE ACESSO: PRIORITÁRIO ( ) INTERMEDIÁRIO ( ) RAZOÁVEL ( )

3 – ATENDIMENTO DA SOLICITAÇÃO			
Servidor (a) Declara estar de acordo com os perfis solicitados e ciente da utilização.		Informática: Declara que nesta data o cadastro fora efetuado.	
Data: ____/____/_____	Assinatura:	Data: ____/___/_____	Assinatura:

ANEXO II – IN STI Nº 001

TERMO RESPONSABILIDADE AGENTE INTERNO

ACESSO AO SISTEMA DE INFORMÁTICA E INTERNET

_____,CPF N º._____,

Cargo:_____ DECLARA haver solicitado acesso ao (s) sistema(s)/site (s) relacionado (s) no anexo I.

Comprometendo-me a:

1. Acessar o (s) sistema (s) informatizado (s) somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas na instrução normativa que rege os acessos a sistemas;
2. Não revelar fora do âmbito profissional fato ou informação de qualquer natureza de que tenha conhecimento por força de suas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial;
3. Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;
4. Não ausentar-se da estação de trabalho sem encerrar a sessão de uso do sistema, garantindo assim a impossibilidade de acesso indevido por terceiros ou dano ao sistema por desligamento incorreto;
5. Não revelar senha de acesso ao (s) sistema (s) adotando cuidados necessários para que permaneça somente de seu conhecimento;
6. Responder, em todas as instâncias, pelas consequências de suas ações ou omissões que possam pôr em risco ou comprometer a exclusividade de conhecimento da senha de acesso e das informações institucionais a que tenha acesso.

Declara, ainda, estar plenamente esclarecido e consciente que:

7. É de sua responsabilidade cuidar da integridade, confidencialidade e disponibilidade dos dados, informações contidas nos sistemas, devendo comunicar por escrito à chefia imediata ou a Controlaria Geral Municipal, quaisquer indícios ou possibilidades de irregularidades, de desvios ou falhas identificadas nos sistemas, sendo proibida a exploração de falhas ou vulnerabilidades porventura existentes;

8. O acesso à informação não me garante direito sobre ela, nem me confere autoridade para liberar acesso a outras pessoas;

9. Constitui descumprimento de normas legais, regulamentares e quebra de sigilo funcional divulgar dados obtidos dos sistemas aos quais tenho acesso para outros servidores não envolvidos nos trabalhos executados;

10. Devo alterar minha senha, sempre que obrigatório ou que tenha suposição de descoberta por terceiros, não usando combinações simples que possam ser facilmente descobertas;

11. Respeitar as normas de segurança e restrições de sistema impostas pelos sistemas de segurança implantados na instituição (tais como direitos de acesso a arquivos, diretórios e recursos disponíveis no ambiente da instituição, etc.)

12. Cumprir e fazer cumprir os dispositivos da Política de Segurança da Informação, de suas diretrizes, bem como deste Termo de Responsabilidade.

13. Ressalvadas as hipóteses de requisições legalmente autorizadas, constitui infração funcional e penal a revelação de segredo do qual me apropriei em razão do cargo.

14. Sendo crime contra a administração pública, a divulgação a quem não seja servidor inserido diretamente na relação de serviço, das informações do (s) sistema (s) ao (s) qual (is) tenho acesso, estando sujeito às penalidades previstas em lei.

15. Sem prejuízo da responsabilidade penal e civil, e de outras infrações disciplinares, constitui falta de zelo e dedicação às atribuições do cargo e descumprimento de normas legais e regulamentares, não proceder com cuidado na guarda e utilização de senha ou emprestá-la a outro servidor, ainda que habilitado.

16. Constitui infração funcional e penal inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos dos sistemas ou bancos de dados da Administração Pública, com o fim de obter vantagem indevida para si ou para

outrem ou para causar dano, bem como modificar ou alterar o sistema de informações ou programa de informática sem autorização ou sem solicitação de autoridade competente, ficando o infrator sujeito as punições previstas no Código Penal Brasileiro, conforme responsabilização por crime contra a Administração Pública.

Declaro, nesta data, ter ciência e estar de acordo com os procedimentos acima descritos, comprometendo-me a respeitá-los e cumpri-los plena e integralmente.

____ de _____ de 20____.

Nome/Assinatura do Servidor (a) Usuário

Matricula Funcional nº _____

Nome/Assinatura do Responsável pelo Setor de TI

Matricula Funcional nº _____

ANEXO III – STI Nº 001

TERMO DE RESPONSABILIDADE – AGENTE EXTERNO

TERMO DE RESPONSABILIDADE PARA USO DE EQUIPAMENTO DE TERCEIROS NA REDE COORPORATIVA DOS ÓRGÃOS DA ADMINISTRAÇÃO DIRETA OU INDIRETA	
IDENTIFICAÇÃO DO AGENTE: Nome Completo: CI/RG Nº CPF/MF Nº	
Vinculo do Agente: ( ) Efetivo ( ) Comissionado ( ) Prestador de Serviços **Órgão/Empresa que representa:** Nome: CNPJ/MF:	
JUSTIFICATIVA/FINALIDADE PARA USO DO EQUIPAMENTO: Em _____/_____/_____ _____ Agente Solicitante	
PRAZO: Indeterminado ( ) não ( ) sim Data e Hora de Início Data e Hora Final: __/__/___ __:___ __/__/__ __:__	
INFORMAÇÕES TÉCNICAS DO EQUIPAMENTO	
Sistema Operacional:	**Modelo:**
MAC ADDRESS:	**MAC ADDRES:**

PERMITIDO / RESPONSABILIDADE DO AGENTE:

Declara estar ciente das recomendações de segurança para utilização do equipamento na rede coorporativa do órgão, assumindo inteira responsabilidade pela guarda e zelo do equipamento, pela legalidade de software nele instalados e por quaisquer incidentes de segurança decorrentes da utilização deste equipamento na rede.

Em ____/____/_____ _____

Usuário

PERMITENTE / SETOR DE TECNOLOGIA DA INFORMAÇÃO:

Declara-se ciente da demanda demonstrada, e na condição de legítimo representante do Setor de Tecnologia da Informação deste órgão, expressa ANUÊNCIA para que o compromitente faça uso da estrutura de TI, pelo prazo fixado neste termo, nas seguintes **condições:**

–

–

–

–

–

DAS RECOMENDAÇÕES DE SEGURANÇA E PROTEÇÃO DAS INFORMAÇÕES PÚBLICAS:

1. O acesso à rede corporativa deste órgão está condicionada INSTALAÇÃO prévia de antivírus no equipamento a ser utilizado, FORA da rede do órgão.
2. Ao ingressar na rede, o usuário deve sempre mantê-lo ATIVADO e ATUALIZADO, durante toda a permanência do equipamento na rede.
3. Sempre instalar as correções de segurança do Sistema Operacional (Windows, Linux, MacOs, etc), no equipamento, antes de ingressar na rede.
4. Não realizar qualquer tipo de compartilhamento de pastas ou arquivos no equipamento.
5. Não executar qualquer tipo de software para varredura de rede, espionagem ou escuta de tráfego de informações.
6. A responsabilidade sobre a segurança física do equipamento e de todos os arquivos, aplicações e backups nele armazenados, bem como de qualquer tipo de problema que este venha a apresentar durante o seu uso no ambiente da rede corporativa, é de inteira responsabilidade do proprietário do equipamento.
7. O Setor de Tecnologia de Informação deste órgão pode, a qualquer momento, bloquear o acesso do equipamento à rede, se detectada não conformidade com as normas de segurança.

Em ___/___/_____ _____

Administrador da Rede de T.I.

Matricula Funcional nº _____

ANEXO IV – IN STI Nº 001

TERMO DE RESPONSABILIDADE

ACESSO REMOTO À REDE CORPORATIVA DA ADMINISTRAÇÃO

1. JUSTIFICATIVA: _____

2. _____, inscrito(a) no CPF nº _____ / matrícula nº _____ (campo obrigatório para servidor), doravante denominado simplesmente USUÁRIO REMOTO, ao acessar remotamente a rede corporativa da(o)_____(órgão da administração direta ou indiret), disponível pelo acesso concedido pelo seu Setor de Tecnologia da Informação, aceita as regras e condições constantes do presente Termo.

3. O objetivo deste Termo de Responsabilidade é prover a necessária e adequada proteção às informações produzidas ou custodiadas pela(a) _____(órgão da administração direta ou indireta), que não sejam de domínio público, às quais o USUÁRIO REMOTO tenha acesso de forma autorizada e em razão de suas atividades afetas aos trabalhos realizados, acordos, convênios ou instrumentos congêneres, decisão administrativa ou em decorrência de direitos e garantias constitucionais e legais.

4. O USUÁRIO REMOTO está sujeito às diretrizes, normas e procedimentos de segurança da informação descritos nesta Instrução Normativa e demais normas legais vigentes relativas à Política de Segurança da Informação e Comunicação da administração municipal, direta e/ou indireta.

5. O termo “informações produzidas ou custodiadas pelos órgãos da administração direta e/ou indireta que não sejam de domínio público” abrange todos os dados e informações restritos ao órgão, armazenados em meio digital.

6. O USUÁRIO REMOTO se compromete a não vender, divulgar, reproduzir, disponibilizar de qualquer forma, por qualquer meio, no todo ou em parte, as informações produzidas ou custodiadas pelo órgão e mencionadas no item 4, que não sejam de domínio público, de que tiver conhecimento ou que lhe forem reveladas.

7. O USUÁRIO REMOTO fica ciente que eventuais informações pessoais a que tenha acesso, são absolutamente sigilosas, não podendo, em hipótese alguma, serem utilizadas fora da circunscrição de trabalho.

8. O USUÁRIO REMOTO se obriga a informar imediatamente ao órgão qualquer violação das regras de responsabilidade estabelecidas neste Termo de que tenha conhecimento, independentemente da existência de dolo, bem como qualquer divulgação ou reprodução de informações abrangidas por este Termo decorrente de exigência por autoridade competente, mediante ordem judicial ou administrativa.

9. O USUÁRIO REMOTO fica ciente de que existe o registro da conexão, sendo de sua inteira responsabilidade quaisquer atos indevidos envolvendo sua conta de acesso durante este período de conexão.

10. O USUÁRIO REMOTO se compromete a utilizar os recursos e as informações, em razão do acesso disponibilizado, apenas e exclusivamente para o subsídio dos trabalhos relativos às suas atribuições de interesse da administração.

11. O USUÁRIO REMOTO se compromete ainda a não utilizar o acesso disponibilizado para qualquer outra atividade que contrarie alguma lei ou norma municipal, estadual, federal ou internacional aplicável, bem como nunca acessar ou tentar o acesso a recursos não autorizados ao seu perfil.

12. No caso de qualquer descumprimento, por ação ou omissão, das regras e condições constantes deste termo, o USUÁRIO REMOTO estará sujeito às sanções cabíveis, administrativas, cíveis e criminais, na forma da lei, assegurados o contraditório e a ampla defesa.

13. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor a partir da sua assinatura e enquanto perdurar a natureza sigilosa ou restrita da informação, inclusive após a cessação da razão que ensejou o acesso à informação.

14. Vigência: ___/___/_____ a ___/___/_____

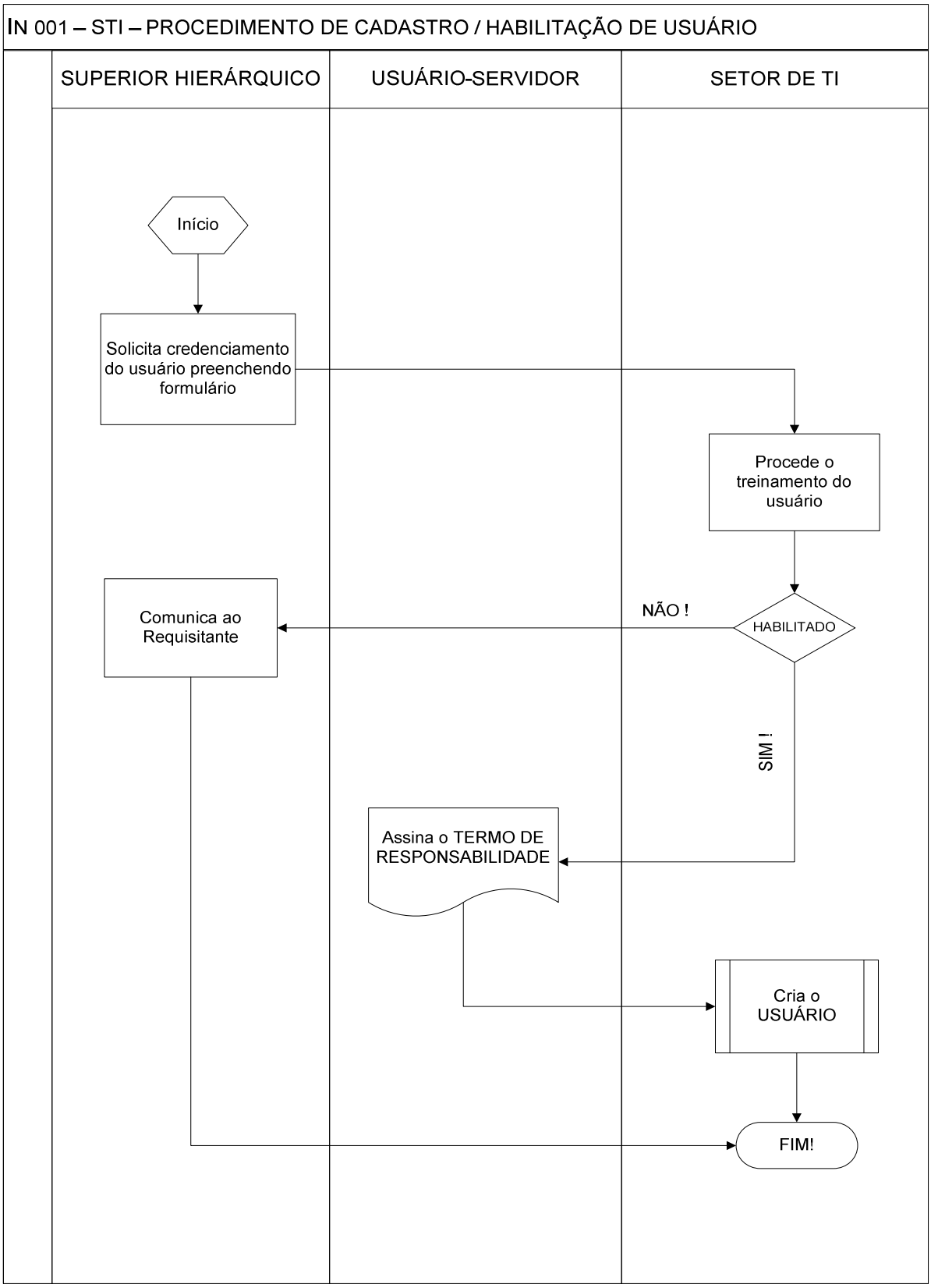
E, por aceitar as regras e condições nele constantes, o USUÁRIO REMOTO assina o presente Termo de Responsabilidade.

_____, _____ de _____ de _____.
(Local)

_____
[ASSINATURA DO USUÁRIO REMOTO]

_____
[ASSINATURA DO GESTOR]

ANEXO V – IN STI Nº 001



ANEXO VI – IN STI Nº 001

IN 001 – STI – PROCEDIMENTO DE DESABILITAÇÃO DE USUÁRIO