ESTADO DO RIO GRANDE DO SUL
PREFEITURA MUNICIPAL DE SANT'ANA DO LIVRAMENTO
"Palácio Moysés Vianna"
Unidade Central de Controle Interno

INSTRUÇÃO NORMATIVA UCCI	**001/2011**	Versão 01
ASSUNTO: REGULAMENTAÇÃO DOS PROCEDIMENTOS DE APOIO TÉCNICO, ADMINISTRATIVO E OPERACIONAL DO SISTEMA DE INFORMAÇÕES	Data:11/08/2011	Pág. 1/6

A PRESENTE INSTRUÇÃO NORMATIVA FOI ELABORADA EM CONJUNTO ENTRE ESTA CONTROLADORIA MUNICIPAL E O DEPARTAMENTO DE TECNOLOGIA DE INFORMAÇÃO.

A – OBJETIVO

A presente Instrução Normativa tem por objetivo principal permitir a ampla e legítima atuação do **DTI – Departamento de Tecnologia de Informação**, de modo a fornecer o eficiente e rápido acesso a informações; vigilância do sistema de informações; integridade e veracidade da informação; garantia de segurança de guarda e acesso a informação; haja vista a necessidade inarredável desta Unidade de Controle Interno ter acesso à informação de boa qualidade, fidedigna, objetiva e clara, essenciais para a tomada de decisões, bem como permitir a otimização de todo o sistema de informação da Administração Pública, além de definir novos procedimentos na área da informática.

B – LEGISLAÇÃO

QUADRO ANEXO DA LEGISLAÇÃO RELACIONADA À SEGURANÇA DA INFORMAÇÃO:

- Dispositivos Legais de Caráter Federal;
- Legislação Específica de Caráter Federal;
- Legislação Específica de Caráter Estadual/Distrital;
- Legislação Específica de Caráter Municipal;
- Normas Técnicas.

C – EXPOSIÇÃO DE MOTIVOS

Sistemas de Informação é a expressão utilizada para descrever um sistema automatizado ou manual, que envolve pessoas, máquinas, e métodos para organizar, coletar, processar e distribuir dados para os usuários do sistema envolvido. Para uma boa informação é necessário existir um conjunto de características para que esse fundamental instrumento de trabalho realmente atenda as necessidades dos gestores, como agilidade e confiabilidade.

O sistema é dividido em subsistemas que abrangem as mais diversas áreas da Administração: licitações, distribuição de material, controle de almoxarifado, patrimônio, contabilidade, pessoal, folha de pagamento, financeiro, orçamentário e outros. O Departamento de Tecnologia de Informação cruza, organiza, controla e fiscaliza esses subsistemas, o que leva a uma abordagem sistemática integrativa, envolvendo questões de planejamento estratégico da Administração.

Cabe ao DTI implementar novas tecnologias computacionais, a fim de melhorar o sistema de informações que integra as diversas unidades da Prefeitura, de conformidade com o que dispõe a CF, Art. 37, § 7º, tendo em vista a responsabilidade dos agentes públicos e do Administrador Público perante a comunidade, zelando para que sua gestão seja profícua e transparente.

A vulnerabilidade da rede Municipal tem se mostrado atingida, segundo recentes Auditorias desta UCCI nesta área, cresce em ritmo mais acelerado do que as atualizações e correções dos Sistemas de Informação, haja vista a falta de regulamentação para a legítima atuação do DTI. Apesar dos antivírus e *firewall* (para barrar invasões externas) estarem instalados, isso não tem se mostrado suficiente para que o sistema esteja livre de ataques combinados, vazamento de informações, utilização indevida da rede ou fraudes, motivos pelos quais se faz necessário o apoio imediato a atuação vigilante do DTI.

A complexidade das estruturas da Administração Municipal, em função dos números de periféricos, banco de dados e outros aplicativos, exige conhecimento técnico especializado e específico para proteção de toda a infraestrutura. Cada usuário é um ponto fixo nas redes IP de alta velocidade, pois estão sempre conectados *on-line* e, se não for a atuação do DTI, acabam nem percebendo quando são vítimas de um ataque. Por esse motivo, o gerenciamento e a gestão da segurança são duas modalidades apontadas como as principais fontes de atenção, merecendo adequados investimentos da área de Tecnologia da Informação.

D – ÂMBITO DE APLICAÇÃO

Todos os Órgãos/Unidades que trabalharem com banco de dados públicos e estiverem ligados à rede Intranet, Internet ou utilizando equipamentos de informática no âmbito da Administração Direta do Município.

E – CONSIDERAÇÕES GERAIS

01 – Os procedimentos estabelecidos nesta Instrução Normativa entrarão em vigor a partir de 12 de agosto de 2011.

02 – A entrada em vigor desta IN tornará sem efeito procedimentos anteriores, naquilo em que, especificamente, divergirem dos procedimentos descritos nesta IN.

03 – Os procedimentos anteriores que não forem atingidos pelas alterações ora introduzidas permanecerão, normalmente, em vigor.

04 – Define-se **DTI** como órgão técnico central da Prefeitura, destinado a prover apoio técnico, administrativo e operacional na área de informática, fornecendo suporte de software, de hardware, dentro do possível e serviços de computação relativos às atividades de pesquisa, administração, suporte e apoio ao usuário.

05 – Cabe ao **DTI** implementar novas tecnologias computacionais, a fim de melhorar o sistema de informações e vigilância que integram as diversas unidades da Prefeitura.

F – PROCEDIMENTO E ATRIBUIÇÕES GERAIS

Compete ao DTI :

01 – Desenvolver programas visando a racionalização dos fluxos administrativos e das rotinas, com atendimento descentralizado, visando maior transparência, adequação à LRF e à LC 131, redução de custos e despesas desnecessárias ou impróprias ao plano de desenvolvimento de informática.

02 – Criar e/ou excluir usuários de acesso à Internet, bem como de acesso aos computadores, criando e identificando sistema de segurança através de senhas de acesso:

a) cada usuário deverá usar uma senha pessoal e intransferível, através da qual será identificado, junto ao DTI, para fins de responsabilização administrativa, cível e penal, no desempenho de suas respectivas atribuições, quando na utilização do Sistema de Informações;

b) haja vista a impossibilidade de responsabilização administrativa dos estagiários, estes receberão senha própria, porém, vinculada, a liberação de acesso, à autorização do servidor responsável pela supervisão do estágio curricular, respondendo, este, por quaisquer irregularidades e ilegalidades praticadas pelo estagiário no âmbito da Administração Municipal, independente da responsabilidade cível e penal;

c) o vínculo de supervisão entre o servidor e o estagiário será formalizado, por escrito, e obrigatoriamente designado pelo Chefe de Gabinete ou pelo Secretário da pasta, devendo, antes de qualquer acesso à rede ou ao Sistema de Informações, ser comunicado ao DTI, para fins de regularização das suas atividades através do registro de senha;

d) o nível de acessibilidade de cada usuário aos Serviços de Informação, definidos pelas senhas, deverá ser estabelecido pelos Chefes de setor, devendo ser solicitado, por escrito, através do Secretário da Pasta, ao DTI;

e) é competência exclusiva do DTI parametrizar os acessos, nas mais diversas formas (consulta, alteração ou exclusão de dados), ao Sistema de Informações, através das Autorizações Eletrônicas, solicitadas pelos Secretários;
f) nenhum acesso ao Sistema de Informações será permitido sem que o usuário possua senha cadastrada junto ao DTI.

03 – Monitorar os usuários quando o sistema de *proxy* informar discrepância de tráfego na rede ou identificar acesso a sites impróprios ao serviço público, cabendo ao DTI a verificação e constatação, via aceso remoto, ou *in loco* na máquina identificada, sem a necessidade de prévia autorização, comunicando à UCCI quando identificada ilegalidade ou irregularidade na utilização da rede, para fins de responsabilização administrativa, cível ou penal quando for o caso.

04 – Proporcionar a análise crítica do sistema organizacional com a aferição dos fatores de desenvolvimento, resultando num relatório circunstanciado e objetivo sobre as potencialidades diagnosticadas, oferecendo as possíveis soluções dos problemas apurados. Cópias dos referidos relatórios deverão ser encaminhados, sempre que emitidos, por meio digital, à UCCI, para fins de acompanhamento dos resultados.

05 – Estimular as iniciativas produtivas de cada setor, com o enfoque na eficiência, potencializando os resultados dos dados e informações atinentes a cada um, considerando o contexto geral.

06 – Assessorar e contribuir para a construção e efetivação das políticas e do planejamento estratégico de Tecnologia da Informação.

07 – Planejar, liderar, fiscalizar e apoiar os processos de implantação de Tecnologia da Informação, sem o que nenhum usuário poderá instalar ou executar aplicativo nocivo a segurança da rede ou instrumento de informação, em qualquer equipamento da Administração Direta, sob pena de responsabilidade administrativa e, em caso de prejuízo, responsabilização penal ou cível, conforme a gravidade do ato.

08 – Gerenciar e executar o planejamento, especificação, desenvolvimento, implantação, operação e a manutenção de serviços, sistemas de informação e infra-estrutura de Tecnologia de Informação.

09 – Prestar serviços de atendimento e suporte aos usuários para plena utilização dos recursos computacionais e de sistemas de informação, não podendo serem praticados, pelos usuários, quaisquer atos invasivos, tanto do sistema como dos *hardwares***,** sem prévia autorização do DTI.

10 – Desenvolver conhecimento tecnológico, através de projetos, na busca de soluções inovadoras na área de Tecnologia da Informação, para melhoria da qualidade dos serviços prestados pela Administração Direta.

11 – Elaborar e desenvolver programas e treinamentos de capacitação de pessoal na área de Tecnologia da Informação.

12 – Articulação, elaboração e acompanhamento dos planos estratégicos e operacionais do Departamento, juntamente com os demais setores, na solução das demandas internas e externas.

13 – Compete ao DTI identificar oportunidades e demandas na área da TI e desenvolver ações e projetos de conteúdo tecnológico inovador que tragam como benefício agregação de valor para o DTI, à Administração Direta e à sociedade.

F – PROCEDIMENTOS E ATRIBUIÇÕES ESPECÍFICAS

Compete ao DTI:

01 – Definição, padronização e gerenciamento dos modelos de informação da Administração Direta; planejamento, análise, desenvolvimento, testes, implantação e manutenção de sistemas de informação; monitoramento da utilização dos sistemas; apoio aos usuários na utilização dos sistemas de informação; resolução de problemas relativos aos sistemas implantados.

02 – Sistematização, organização, preservação e auditoria de processos, metodologias e documentos através de articulação e interação pró-ativa com seu grupo, devendo ser informada, por escrito, a identificação de qualquer irregularidade ou ilegalidade à UCCI.

03 – Criar mecanismos de aproximação das esferas decisórias da Administração Direta visando um posicionamento ativo nas decisões de TI.

04 – Preparar manuais de serviço na área de TI, elaborar minutas de informações, pareceres, exposição de motivos, relatórios, etc. Coordenar, orientar e controlar tarefas especifica de processamento de dados.

05 – Todos os diálogos e documentos que tramitem na Intranet (achat) serão considerados instrumentos formais e probantes, quando ratificados pela Chefia do Setor ou apreendidos em auditoria pelo DTI ou pela UCCI.

CONDUTAS EXIGÍVEIS POR LEI, PASSÍVEIS DE RESPONSABILIZAÇÃO

1. É obrigatório tratamento sigiloso das informações fiscais e tributárias dos contribuintes e das autoridades públicas (sigilo perante terceiros e não em face da Administração Pública).

2. Devem ser mantidas sob sigilo as informações acessadas no exercício do serviço público (empresas públicas e sociedades de economia mista).

3. É proibido à autoridade pública de prestar consultoria valendo-se de informações não divulgadas publicamente a respeito de programas ou políticas do órgão ou da entidade da Administração Pública Municipal a que esteve vinculado ou com que tenha tido relacionamento direto e relevante nos seis meses anteriores ao término do exercício de função pública.

4. É proibido a alteração de documentos sem autorização legal ou da Autoridade Competente, visando a proteção da integridade das informações públicas.

5. É proibido retirar da repartição documento ou qualquer outro bem sem a devida autorização, visando a proteção da disponibilidade das informações públicas.

6. É obrigatório conferir publicidade aos atos administrativos, quando determinado por lei, salvo os sigilosos, visando a proteção da disponibilidade das informações públicas e garantia da publicidade das informações de interesse da coletividade.

7. É obrigatório zelar pela conservação, evitando causar dano a qualquer bem pertencente ao patrimônio público, deteriorando-o, por descuido ou má vontade, não constituindo apenas uma ofensa ao equipamento e às instalações ou ao Estado, mas configurando crime tipificado no Código Penal.

8. É proibido aos servidor que se valer ou permitir dolosamente que terceiros tirem proveito indevido de informação obtida em função do cargo, para lograr, proveito pessoal ou de outrem, visando a proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.

9. É proibido revelar segredo de que teve conhecimento em função do cargo ou emprego, visando a proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.

10. É dever do servidor guardar sigilo sobre assunto da repartição.

11. E dever do servidor que exerce funções específicas de Controle Interno na UCCI de guardar sigilo sobre dados e informações obtidos em decorrência do exercício de suas funções e pertinentes aos assuntos sob sua fiscalização, utilizando-os, exclusivamente, para a elaboração de pareceres e relatórios.

12. É prerrogativa da Unidade Central de Controle Interno requisitar informações, exames, perícias e documentos de autoridades da Administração Pública Direta ou Indireta e do Poder Legislativo Municipal, e ter acesso incondicional a qualquer banco de dados de caráter público ou relativo a serviço de relevância pública, bem como a fiscalização do uso dessas informações, visando a proteção da disponibilidade e sigilo das informações constantes nos registros públicos.

13. Compete ao DTI coordenar a atividade de segurança da informação, com o auxílio da UCCI.

14. Serão classificados como “sigilosos” os procedimentos de investigação de condutas antiéticas relativas ao Sistema de Informações. Concluída a investigação e após a deliberação da Comissão de Investigação, o processo será encaminhado à Autoridade Instauradora.

DISPOSIÇÕES FINAIS

01 – A entrada em vigor desta IN revoga procedimentos anteriores naquilo em que, especificamente, divergirem dos procedimentos descritos nesta.

02 – Os procedimentos anteriores que não forem atingidos pelas alterações ora introduzidas permanecerão, normalmente, em vigor.

03 – Acompanha a presente IN, o Anexo I – Quadro dos Dispositivos Legais relacionados à Segurança da Informação.

Controle Interno, em Sant'Ana do Livramento, 12 de agosto de 2011.

API **Teddi Willian Ferreira Vieira** – Matr. 218758
Assessoria Jurídica – UCCI

Adm. **Sandra Helena Curte Reis** – CRA/RS 19.515
Chefia da UCCI

Ciente em ____/____/2011

_____
Wainer Viana Machado
Prefeito Municipal

ANEXO I

Dispositivos Legais de Caráter Federal
Legislação Específica de Caráter Federal
Legislação Específica de Caráter Estadual/Distrital
Legislação Específica de Caráter Municipal
Normas Técnicas
Projetos de Leis

Quadro dos dispositivos legais de caráter federal, relacionados à segurança da informação:

Dispositivo	Mandamento Legal	Aspecto da SI
Constituição Federal, art. 5º, inciso X.	Direito à privacidade.	Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.
Constituição Federal, art. 5º, inciso XII.	Direito à privacidade das comunicações.	Sigilo dos dados telemáticos e das comunicações privadas.
Constituição Federal, art. 5º, inciso XIV.	Resguardo do sigilo profissional em caso de ofício que exige a ampla confidência no interesse de quem confidencia, como advogados, padres, médicos, psicólogos, etc.	Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.
Constituição Federal, art. 5º, inciso XXXIII e art. 37, § 3º, inciso II.	Direito à informação e ao acesso aos registros públicos.	Disponibilidade das informações constantes nos órgãos públicos.
Constituição Federal, art. 5º, inciso XXXIV.	Direito de petição e de obtenção de certidões em repartições públicas.	Disponibilidade das informações constantes nos órgãos públicos.
Constituição Federal, art. 23, incisos III e IV.	Dever do Estado de proteger os documentos e obras.	Proteção da integridade, da autenticidade e da disponibilidade das informações pelo Estado.
Constituição Federal, art. 216, § 2º.	Obrigação da Administração Pública de promover a gestão documental.	Proteção da integridade, da autenticidade, da disponibilidade e do sigilo das informações constantes nos órgãos e entidades integrantes da Administração Pública.
Constituição Federal, art. 37, caput.	Vinculação da Administração Pública aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência.	Quanto melhor a gestão das informações, mais eficiente será o órgão ou entidade, daí a necessidade de implantação de uma Política de Segurança da Informação.
Constituição Federal, art. 37, § 6º e Código Civil, art. 43.	Responsabilidade objetiva do Estado e das pessoas de direito privado prestadoras de serviços públicos pelos danos causados a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.	Responsabilidade objetiva do Estado por dano decorrente da má gestão das informações pelos órgãos e entidades da Administração Pública e pessoas de direito privado prestadoras de serviços públicos.
Constituição Federal, art. 37, § 7º.	Lei disporá sobre os requisitos e as restrições ao ocupante de cargo ou emprego da administração direta e indireta que possibilite o acesso a informações privilegiadas.	Necessidade de regulamentação do acesso a informações privilegiadas.
Consolidação das Leis do Trabalho – CLT, art. 482, alínea g.	Rescisão de contrato de trabalho de empregado que viola segredo da empresa.	Proteção das informações sigilosas acessadas no exercício de emprego público (empresas públicas e sociedades de economia mista).

Código de Conduta da Alta Administração, art. 5º, § 4º.	Caráter sigiloso das informações pertinentes à situação patrimonial da autoridade pública.	Sigilo das informações fiscais e tributárias das autoridades públicas (sigilo perante terceiros e não em face da Administração Pública)..
Código de Conduta da Alta Administração, art.14, inciso II.	Proibição da autoridade pública de prestar consultoria valendo-se de informações não divulgadas publicamente a respeito de programas ou políticas do órgão ou da entidade da Administração Pública Federal a que esteve vinculado ou com que tenha tido relacionamento direto e relevante nos seis meses anteriores ao término do exercício de função pública.	Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.
Decreto nº 1.171/94 (Código de Ética do Servidor Público), alínea "h" do inciso XV da Seção II.	Proibição de alteração de documentos que devam ser encaminhados para providências.	Proteção da integridade das informações públicas.
Decreto nº 1.171/94 (Código de Ética do Servidor Público), alínea "l" do inciso XV da Seção II.	Proibição de retirar da repartição documento ou qualquer outro bem.	Proteção da disponibilidade das informações públicas.
Decreto nº 1.171/94 (Código de Ética do Servidor Público), inciso X da Seção I.	Deixar o servidor público ou qualquer pessoa à espera de solução que compete ao setor em que exerça suas funções, permitindo a formação de longas filas, ou qualquer outra espécie de atraso na prestação do serviço, não caracteriza apenas atitude contra a ética ou ato de desumanidade, mas principalmente grave dano moral aos usuários dos serviços públicos.	Proteção da disponibilidade das informações públicas.
Decreto nº 1.171/94 (Código de Ética do Servidor Público), inciso VII da Seção I.	Obrigação moral de conferir publicidade aos atos administrativos, salvo os sigilosos.	Proteção da disponibilidade das informações públicas e garantia da publicidade das informações de interesse da coletividade.
Decreto nº 1.171/94 (Código de Ética do Servidor Público), inciso IX da Seção I.	Causar dano a qualquer bem pertencente ao patrimônio público, deteriorando-o, por descuido ou má vontade, não constitui apenas uma ofensa ao equipamento e às instalações ou ao Estado, mas a todos os cidadãos.	Proteção da integridade do patrimônio público, a exemplo de equipamentos, materiais, áreas e instalações.
Decreto nº 1.171/94 (Código de Ética do Servidor Público), alínea "e" do inciso XIV da Seção II.	Dever de aperfeiçoar o processo de comunicação com os usuários para bem servi-los.	Disponibilidade das comunicações.
Código de Propriedade Industrial, art. 75.	O pedido de patente originário do Brasil cujo objeto interesse à defesa nacional será processado em caráter sigiloso.	Sigilo das patentes de interesse da defesa nacional.
Código de Defesa do Consumidor, arts. 43 e 44.	Direito de acesso do consumidor às suas informações pessoais arquivadas em bancos de dados e direito de retificação das informações incorretas.	Garantia da integridade e disponibilidade das informações dos consumidores arquivadas em bancos de dados.

Código Penal, art. 151.	Pena de detenção de um a seis meses ou multa por crime de violação de correspondência fechada dirigida a outrem, sonegação ou destruição de correspondência, e violação de comunicação telegráfica, radioelétrica ou telefônica.	Proteção do sigilo, integridade e disponibilidade das informações de caráter pessoal veiculadas através dos meios de comunicação.
Código Penal, art. 152.	Pena de detenção de três meses a dois anos pelo crime de desvio, sonegação, subtração, supressão ou revelação de conteúdo de correspondência comercial, abusando da condição de sócio ou empregado.	Proteção do sigilo e da disponibilidade das informações dos estabelecimentos comerciais.
Código Penal, art. 153.	Pena de 1 a 4 anos e multa por crime de divulgação de documento confidencial contido ou não nos sistemas ou bancos de dados da Administração Pública.	Proteção do sigilo das informações classificadas constantes nos sistemas ou bancos de dados da Administração Pública.
Código Penal, art. 154.	Pena de três meses a um ano, ou multa por crime de violação de segredo profissional.	Proteção do sigilo das informações conhecidas em razão de função, ministério, ofício ou profissão.
Código Penal, art. 184, § 3º.	Pena de dois a quatro anos por crime de violação de direito autoral mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema.	Proteção da autenticidade.
Código Penal, art. 297.	Pena de dois a seis anos, e multa por crime de falsificação de documento público.	Proteção da integridade e autenticidade dos documentos públicos.
Código Penal, art. 298.	Pena de um a cinco anos, e multa por crime de falsificação de documento particular.	Proteção da integridade e autenticidade dos documentos particulares.
Código Penal, art. 305.	Pena de 2 a 6 anos e multa por crime de supressão, destruição ou ocultação de documento público ou particular.	Proteção da disponibilidade e integridade das informações constantes nos órgãos e entidades públicos.
Código Penal, art. 307.	Pena de três meses a um ano, ou multa por crime de falsa identidade.	Proteção da autenticidade.
Código Penal, art. 313-A.	Pena de 2 a 12 anos e multa por crime de inserção de dados falsos em sistema informatizado ou banco de dados da Administração Pública, alteração ou exclusão de dados corretos.	Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.
Código Penal, art. 313-B.	Pena de 3 meses a 2 anos e multa por crime de modificação ou alteração não autorizada de sistemas de informações.	Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.
Código Penal, art. 314.	Pena de um a quatro anos por crime de extravio, sonegação ou inutilização de livro ou documento de que tem a guarda em razão do cargo.	Proteção da disponibilidade das informações constantes nos órgãos e entidades públicos.
Código Penal, art. 325.	Pena de seis meses a dois anos, ou multa por crime de violação de	Proteção das informações sigilosas acessadas no exercício de cargo,

	sigilo funcional.	função ou emprego público.
Código Processo Penal, art. 20.	Sigilo do inquérito policial	Proteção de informações sigilosas.
Código Processo Penal, art. 207.	Proibição de depor das pessoas que, em razão de função, ministério, ofício ou profissão, devam guardar segredo, salvo se, desobrigadas pela parte interessada, quiserem dar o seu testemunho.	Proteção do sigilo profissional.
Código Processo Penal, art. 745.	Sigilo do processo de reabilitação do condenado.	Proteção de informações sigilosas relacionadas ao condenado.
Código Tributário Nacional, art. 198.	Proibição de divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades.	Proteção do sigilo fiscal.
Código de Processo Civil, art. 347, inciso II c/c art.363, inciso IV.	Direito da parte de guardar sigilo profissional.	Proteção da privacidade de seus clientes.
Código de Processo Civil, art. 406, inciso II c/c art.414, § 2º.	Direito da testemunha de guardar sigilo profissional.	Proteção da privacidade de seus clientes.
Lei nº 6.538/78, art. 41.	Pena de detenção de três meses a um ano, ou multa por violação de sigilo profissional por funcionário do serviço postal.	Proteção da privacidade de correspondência.
Lei nº 7.170/83, art. 13.	Pena de três a quinze anos por crime espionagem ou divulgação de informações sigilosas a grupo estrangeiro, ou a organização ou grupo de existência ilegal.	Proteção das informações sigilosas relacionadas à segurança nacional
Lei nº 7.232/84, art. 2o, inciso VIII.	Exigência de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados informatizados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas.	Sigilo dos dados relacionados à intimidade, vida privada e honra, especialmente dos dados armazenados através de recursos informáticos.
Lei nº 7.492/86, art. 18.	Pena de reclusão de 1 a 4 anos e multa por crime de violação de sigilo bancário.	Proteção das informações sigilosas no âmbito das instituições financeiras ou integrantes do sistema de distribuição de títulos mobiliários.
Lei nº 8.027/90, artigo 5º, inciso I.	Pena de demissão para o servidor que se valer ou permitir dolosamente que terceiros tirem proveito de informação obtida em função do cargo, para lograr, proveito pessoal ou de outrem.	Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.
Lei nº 8.027/90, artigo 5º, parágrafo único, inciso V.	Pena de demissão para o servidor que revelar segredo de que teve conhecimento em função do cargo ou emprego.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.
Lei nº 8.112/90, art. 116, inciso	Dever do servidor de guardar sigilo	Sigilo das informações produzidas

VIII.	sobre assunto da repartição.	ou conhecidas no exercício de cargo ou função pública.
Lei nº 8.112/90, art. 132, inciso IX.	Pena de demissão para o servidor que revelar segredo do qual se apropriou em razão do cargo ou função pública.	Proteção das informações sigilosas acessadas no exercício de cargo ou função pública.
Lei nº 8.137/90, art. 3º, inciso I.	Constitui crime funcional contra a ordem tributária punido com pena de 3 a 8 anos e multa extraviar livro oficial, processo fiscal ou qualquer documento, de que tenha a guarda em razão da função; sonegá-lo, ou inutilizá-lo, total ou parcialmente, acarretando pagamento indevido ou inexato de tributo ou contribuição social.	Proteção da disponibilidade de informações para manutenção da ordem tributária.
Lei nº 8.429/92, art.11, incisos III, IV e VII..	Constitui ato de improbidade administrativa revelar fato ou circunstância de que tem ciência em razão das atribuições e que deva permanecer em segredo; negar publicidade aos atos oficiais; e revelar ou permitir que chegue ao conhecimento de terceiro, antes da respectiva divulgação oficial, teor de medida política ou econômica capaz de afetar o preço de mercadoria, bem ou serviço.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público, bem como garantia de publicidade das informações de interesse coletivo ou geral que devem ser divulgadas por ato oficial.
Lei nº 8.429/92, art. 13.	Dever do agente público de apresentar anualmente sua declaração de bens e valores que integram o seu patrimônio pessoal a fim de ser arquivada no serviço de pessoal competente e pena de demissão para o servidor que se recusar a prestar tal informação ou que a prestar falsa.	Disponibilidade de informações pessoais do agente público para o Poder Público e veracidade dos dados.
Lei nº 8.443/92, art. 86, inciso IV.	Dever do servidor que exerce funções específicas de controle externo no TCU de guardar sigilo sobre dados e informações obtidos em decorrência do exercício de suas funções e pertinentes aos assuntos sob sua fiscalização, utilizando-os, exclusivamente, para a elaboração de pareceres e relatórios destinados à chefia imediata.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.
Lei Complementar nº 75/93, art. 8º incisos II e VIII, §§ 1º e 2º.	Competência do Ministério Público da União para requisitar informações, exames, perícias e documentos de autoridades da Administração Pública direta ou indireta e ter acesso incondicional a qualquer banco de dados de caráter público ou relativo a serviço de relevância pública, bem como a responsabilização pelo uso dessas informações.	Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.

Lei nº 8.625/93, art. 26, inciso I, alínea b e inciso II.	Competência do Ministério Público de requisitar informações, exames periciais e documentos de autoridades federais, estaduais e municipais, bem como dos órgãos e entidades da administração direta, indireta ou fundacional, de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios e requisitar informações e documentos a entidades privadas, para instruir procedimentos ou processo em que oficie.	Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.
Lei nº 8.906/94, art. 7º, inciso XIX.	Direito do advogado de resguardar o sigilo profissional.	Proteção da privacidade do cliente do advogado.
Lei nº 9.100/95, art. 67, incisos VII e VIII.	Constitui crime de fraude eleitoral nas eleições municipais as condutas de: (a) obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos; e (b) tentar desenvolver ou introduzir comando, instrução ou programa de computador, capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados utilizado pelo serviço eleitoral.	Proteção da integridade e autenticidade dos sistemas informatizados e das informações neles armazenadas.
Lei nº 9.279/96, art. 195, inciso XI.	Constitui crime de concorrência desleal divulgar, explorar ou utilizar, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato.	Proteção da privacidade das pessoas jurídicas, relacionado ao sigilo de suas informações.
Lei nº 9.296/96, art. 10.	Pena de dois a quatro anos, e multa por crime de interceptação de comunicações telefônicas, de informática ou telemática, ou quebra de segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.	Sigilo dos dados e das comunicações privadas.
Lei nº 9.472/97, art. 3º, inciso V.	O usuário de serviços de telecomunicações tem direito à inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições	Sigilo das comunicações.

	constitucional e legalmente previstas.	
Lei nº 9.472/97, art. 3º, inciso VI.	O usuário de serviços de telecomunicações tem direito à não divulgação, caso o requeira, de seu código de acesso.	Proteção de informações pessoais de caráter sigiloso.
Lei nº 9.472/97, art. 3º, inciso IX.	O usuário de serviços de telecomunicações tem direito ao respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço.	Proteção de informações pessoais de caráter sigiloso.
Lei nº 9.504/97, art. 72.	Pena de 5 a 10 anos pelas condutas de obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos; desenvolver ou introduzir comando, instrução, ou programa de computador capaz de provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral; causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.	Proteção da integridade das informações de caráter eleitoral e dos equipamentos.
Lei nº 9.605/98, art. 62.	Pena de 1 a 3 anos e multa pela conduta de destruir, inutilizar ou deteriorar arquivo, registro, museu, biblioteca, pinacoteca, instalação científica ou similar protegido por lei, ato administrativo ou decisão judicial.	Disponibilidade e integridade de dados e informações.
Lei nº 10.683/03, art. 6º.	Prevê a competência do GSIPR de coordenar a atividade de segurança da informação.	Todos os aspectos da segurança da informação.
Lei n.º 10.703/03, arts. 1º , 2º e 3º, de 18 de julho de 2003.	Incumbe aos prestadores de serviços de telecomunicações na modalidade pré-paga, em operação no território nacional, manter cadastro atualizado de usuários. Os dados constantes do cadastro, salvo motivo justificado, deverão ser imediatamente disponibilizados pelos prestadores de serviços para atender solicitação da autoridade judicial, sob pena de multa de até R$ 10.000,00 (dez mil reais) por infração cometida.	Disponibilidade de dados cadastrais para fins de investigação criminal e sigilo nas demais hipóteses.
Decreto nº 4.801/03, art. 1º, inciso X.	Atribuição da Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo, de formular políticas públicas e diretrizes, aprovar, promover a articulação e acompanhar a implementação dos	Todos os aspectos da segurança da informação.

	programas e ações estabelecidos no âmbito da segurança da informação.	
Decreto nº 5.483/05, arts. 3º e 11.	Dever do agente público de apresentar anualmente sua declaração de bens e valores que integram o seu patrimônio e dever de sigilo por parte da Administração Pública dessas informações.	Disponibilidade de informações pessoais do agente público para o Poder Público e dever de sigilo por parte da Controladoria-Geral da União.
Decreto nº 5.687/06, arts.10 e 13 do Anexo.	Convenção das Nações Unidas contra a Corrupção aprovada pelo Congresso Nacional e promulgada pelo Decreto nº 5.687/06, segundo a qual, cada Estado signatário deve esforçar-se para implementar, entre outras, as seguintes medidas: art. 10: a) instaurar procedimentos ou regulamentações que permitam ao público em geral obter informação sobre a organização, o funcionamento e os processos de adoção de decisões de sua administração pública, com o devido respeito à proteção da intimidade e dos documentos pessoais; b) simplificar procedimentos administrativos a fim de facilitar o acesso do público às informações; c) dar publicidade às informações; - art. 13: a) aumentar a transparência e promover a contribuição da cidadania aos processos de adoção de decisões; b) garantir o acesso eficaz do público à informação.	Disponibilidade das informações públicas ou administrativas e sigilo das informações pessoais constantes nos registros públicos.
Decreto nº 6.029/07, inciso II do art. 1º.	O Sistema de Gestão da Ética do Poder Executivo Federal tem como um de seus objetivos contribuir para a implementação de políticas públicas tendo a transparência e o acesso à informação como instrumentos fundamentais para o exercício de gestão da ética pública.	Disponibilidade das informações constantes nos registros públicos
Decreto nº 6.029/07, art. 10.	Nos trabalhos das Comissões de Ética deverão ser observados os princípios da proteção à honra e à imagem do investigado, bem como proteção à identidade do denunciante, que deverá ser mantida sob reserva se este o desejar.	Sigilo da identidade do denunciante e sigilo do processo para proteção da honra e da imagem do investigado antes da prolação da decisão pela Comissão de Ética.
Decreto nº 6.029/07, art. 13.	Serão classificados como “reservados” os procedimentos de investigação de condutas antiéticas. Concluída a investigação e após a deliberação	Sigilo do processo administrativo por infração ética antes da prolação da decisão e publicidade após o término e aplicação das penalidades.

	da Comissão de Ética, o processo deixará de ser “reservado”.	
Decreto nº 6.029/07, art. 22.	Comissão de Ética Pública manterá banco de dados de sanções aplicadas para fins de consulta antes de novas nomeações.	Disponibilidade, integridade e autenticidade das informações constantes no banco de dados mantido pela Comissão de Ética Pública.

Quadro da legislação específica de caráter federal relacionada à segurança da informação:

Regulamento	Assunto
Lei nº 7.232, de 29 de outubro de 1984.	Dispõe sobre a Política Nacional de Informática, e dá outras providências.
Lei nº 8.248, de 23 de outubro de 1991.	Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências.
Lei nº 9.296, de 24 de julho de 1996.	Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal que dispõe sobre a violação do sigilo de dados e das comunicações telefônicas.
Lei nº 9.472, de 16 de julho de 1997.	Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais.
Lei nº 9.507, de 12 de novembro de 1997.	Regula o direito de acesso a informações e disciplina o rito processual do habeas data.
Lei nº 9.609, de 19 de fevereiro de 1998.	Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.
Lei nº 9.883, de 07 de dezembro de 1999.	Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências.
Lei nº 8.159/91, de 08 de janeiro de 2001.	Dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências.
Lei Complementar 105, de 10 de janeiro de 2001.	Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.
Medida Provisória nº 2.200-2, de 24 de agosto de 2001.	Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.
Lei nº 10.973, de 02 de dezembro de 2004.	Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências.
Lei nº 11.111, de 05 de maio de 2005.	Regula o direito à informação e ao acesso aos registros públicos.
Lei nº 11.419, de 19 de dezembro de 2006.	Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências.
Decreto nº 2.295, 04 de agosto de 1997.	Regulamenta o disposto no art. 24, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Neste caso o processo deverá ser sigiloso, excetuando-se a publicidade das compras governamentais.
Decreto nº 2.556, de 20 de abril de 1998.	Regulamenta o registro previsto no art. 3º da Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.
Decreto nº 3.294, de 15 de dezembro de 1999.	Institui Programa Sociedade da Informação, com objetivo de viabilizar a nova geração da Internet e suas aplicações em benefício da sociedade brasileira.
Decreto nº 3.505, de 13 de junho de 2000.	Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

Decreto de 18 de outubro de 2000.	Cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico, e dá outras providências.
Decreto nº 3.714, 03 de janeiro de 2001.	Dispõe sobre a remessa por meio eletrônico de documentos a que se refere o art. 57-A do Decreto no 2.954, de 29 de janeiro de 1999, e dá outras providências.
Decreto nº 3.996, de 31 de outubro de 2001.	Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.
Decreto nº 4.073, de 03 de janeiro de 2002.	Regulamenta a Lei nº 8.159, de 08 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.
Decreto nº 4.376, de 13 de setembro de 2002.	Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, e dá outras providências.
Decreto nº 4.522, 17 de dezembro de 2002.	Dispõe sobre o Sistema de Geração e Tramitação de Documentos Oficiais - SIDOF, e dá outras providências.
Decreto nº 4.553, de 27 de dezembro de 2002.	Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.
Decreto nº 4.689, de 07 de maio de 2003.	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação – ITI, e dá outras providências.
Decreto nº 4.829, de 03 de setembro de 2003.	Dispõe sobre a criação do Comitê Gestor da Internet no Brasil – CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências.
Decreto de 29 de outubro de 2003.	Institui Comitês Técnicos do Comitê Executivo do Governo Eletrônico e dá outras providências.
Decreto nº 5.301, de 09 de dezembro de 2004.	Institui a Comissão de Averiguação e Análise de Informações Sigilosas, dispõe sobre suas atribuições e regula seu funcionamento.
Decreto nº 5.450, de 31 de maio de 2005.	Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências.
Decreto nº 5.563, de 11 de outubro de 2005.	Regulamenta a Lei nº 10.973, de 02/12/04, que dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo, e dá outras providências.
Decreto nº 5.584, de 18 de novembro de 2005.	Dispõe sobre o recolhimento ao Arquivo Nacional dos documentos arquivísticos públicos produzidos e recebidos pelos extintos Conselho de Segurança Nacional - CSN, Comissão Geral de Investigações - CGI e Serviço Nacional de Informações - SNI, que estejam sob a custódia da Agência Brasileira de Inteligência - ABIN.
Decreto nº 5.772, de 08 de maio de 2006, art. 8º.	Institui na estrutura regimental do Gabinete de Segurança Institucional da Presidência da República o Departamento de Segurança da Informação e Comunicações com diversas atribuições na área de segurança da informação e comunicações.
Decreto nº 6.605, de 14 de outubro de 2008.	Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC.
Instrução Normativa nº 1 do GSI, de 13 de junho de 2008.	Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
Resolução nº 58 do INPI, de 14 de julho de 1998.	Estabelece normas e procedimentos relativos ao registro de programas de computador.
Resolução nº 59 do INPI, de 14 de julho de 1998.	Estabelece os valores das retribuições pelos serviços de registro de programas de computador.
Resolução nº 338 do STF, de 11 de abril de 2007.	Dispõe sobre classificação, acesso, manuseio, reprodução, transporte e guarda de documentos e processos de natureza sigilosa no âmbito do STF.
Resolução nº 140 do TST, de 13	Regulamenta, no âmbito da Justiça do Trabalho, a Lei n° 11.419, de

de setembro de 2007.	19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial.
Resolução nº 22.718/08 do TSE, arts. 18 e 19.	Regula a propaganda eleitoral na internet em campanha nas eleições de 2008.

Quadro da legislação específica de caráter estadual/distrital relacionada à segurança da informação:

Regulamento	Assunto
Lei Distrital nº 3.437, de 09 setembro de 2004.	Dispõe sobre o cadastro dos usuários das empresas ou instituições que locam ou cedem gratuitamente computadores e máquinas para acesso à Internet, no âmbito do Distrito Federal, conhecidas também como “cyber-cafés”.
Lei Estadual de São Paulo nº 12.228, de 11 de janeiro de 2006.	Dispõe sobre os estabelecimentos comerciais que colocam a disposição, mediante locação, computadores e máquinas para acesso à Internet e dá outras providências.
Lei Estadual do Rio Grande do Sul nº 12.698, de 04 de maio de 2007.	Dispõe sobre a proteção da saúde dos consumidores nos estabelecimentos comerciais que ofertam a locação e o respectivo acesso a jogos de computador em rede local, conhecidos como "LAN house" - "Local Área Network" -, e seus correlatos, e dá outras providências, dentre as quais a exigência de cadastramento dos menores de 18 anos que freqüentam o local.
Lei Estadual de São Paulo nº 12.906, de 14 de abril de 2008.	Estabelece normas suplementares de direito penitenciário e regula a vigilância eletrônica, e dá outras providências.
Decreto Estadual do Paraná nº 5.111, de 19 de julho de 2005.	Estabelece diretrizes para o licenciamento de programas de computador de titularidade de entidades da Administração Estadual na Licença Pública Geral da Administração Pública – LPG-AP, e dá outras providências.

Quadro da legislação específica de caráter municipal relacionada à segurança da informação:

Regulamento	Assunto
Lei Municipal de Farroupilha-RS nº 3.087, de 29 de dezembro de 2005.	Dispõe sobre o funcionamento das casas de jogos por computador conhecidos como Lan Houses, e dá outras providências, dentre as quais a exigência de cadastramento dos menores de 18 anos que freqüentam o local.

Quadro de normas técnicas relacionadas à segurança da informação:

Regulamento	Assunto
ISO/IEC TR 13335-3:1998.	Esta norma fornece técnicas para a gestão de segurança na área de tecnologia da informação. Baseada na norma ISO/IEC 13335-1 e TR ISO/IEC 13335-2. As orientações são projetadas para auxiliar o incremento da segurança na TI.
ISO/IEC GUIDE 51:1999.	Esta norma fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos. É aplicável a qualquer aspecto de segurança relacionado a pessoas, propriedades, ao ambiente, ou a uma combinação de um ou mais destes (por exemplo, somente pessoas; pessoas e propriedades; pessoas, propriedades e o ambiente).
ISO/IEC GUIDE 73:2002.	Esta norma fornece definições genéricas de termos de gestão de riscos para a elaboração de normas. Seu propósito é ser um documento genérico de alto nível voltado para a preparação ou revisão de normas que incluam aspectos de gestão de riscos.
ABNT NBR ISO IEC 17799: 2005.	Esta norma é equivalente à ISO/IEC 17799:2005. Consiste em um guia prático que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos de controle e os controles definidos nesta norma têm como finalidade atender aos requisitos identificados na análise/avaliação de riscos.

ABNT NBR ISO/IEC 27001:2005.	Esta norma é usada para fins de certificação e substitui a norma Britânica BS 7799-2:2002. Aplicável a qualquer organização, independente do seu ramo de atuação, define requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão de Segurança da Informação.