Em 27/08/02

Assessoria de Plenário

Ao Protocolo Legislativo para registro e, em seguida à CEOF e CCJ.

02/09/02.

Itamar Pinheiro Lima
Chefe da Assessoria de Plenário

MENSAGEM
Nº458 / 2002

Brasília, 28 de Agosto de 2002.

Excelentíssimo Senhor Presidente da Câmara Legislativa do Distrito Federal,

Tenho a honra de submeter à elevada deliberação dessa Augusta Casa Legislativa o anexo Projeto de Lei, que *"dispõe sobre a prevenção das entidades públicas do Distrito Federal com relação aos procedimentos praticados na área de informática e dá outras providências"*.

O Brasil, nos últimos anos, está seguindo uma tendência mundial de informatização dos serviços em todos os setores da economia, incluindo-se os órgãos e entidades públicas do Distrito Federal. Esta é uma prática que traz inúmeros benefícios para a sociedade, que está sendo preparada para ingressar na era digital, tendo o acesso à informação garantido.

Entretanto, esta tendência traz a necessidade de agregar segurança aos processos realizados. Riscos antes inexistentes tornam-se primordiais de serem tratados, com o objetivo de assegurar a segurança das informações governamentais e dos cidadãos, preservando assim a imagem das instituições.

PROTOCOLO LEGISLATIVO
PL n.º 3133/02
Fls. n.º 01

Exmo Sr.
Deputado JORGE AFONSO ARGELLO
M.D. Presidente da Câmara Legislativa do Distrito Federal
NESTA

O presente Projeto de Lei tem por objetivo definir diretrizes de proteção às informações dos órgãos e entidades públicas do Distrito Federal, independentemente do local em que estejam armazenadas ou do meio em que estejam trafegando.

Faz-se necessário, em todas as esferas de que trata este Projeto de Lei, a adoção de controles que protejam as informações nos seus aspectos de disponibilidade, integridade, confidencialidade e autenticidade.

Assim sendo, diante da importância das informações processadas nos órgãos e entidades da Administração, o Presidente da República editou o Decreto 3.505, de 13 de junho de 2000, instituindo a Política Nacional de Segurança da Informação.

A Administração Pública, em todos os seus níveis e órgãos, processa informações consideradas sensíveis, que requerem uma proteção efetiva, justificando, pois, o estabelecimento de uma política de segurança do material informativo que é armazenado e documentado em seus sistemas de computação.

Neste mesmo sentido a questão de segurança da informação deverá ser reposicionada no âmbito do Governo do Distrito Federal, de modo a receber um tratamento destacado e permanente por meio da "Política de Segurança da Informação dos órgãos e entidades públicas do Distrito Federal".

Nesse contexto, impõe-se a criação de uma legislação específica e mais apropriada. O presente Projeto de Lei pretende evidenciar a política de segurança da informação nos órgãos e entidades públicas do Distrito Federal, tendo os seguintes objetivos: a) dotá-los de instrumentos e recursos tecnológicos que os capacitem a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados e informações; b) eliminar a dependência externa, em relação a sistemas e equipamentos relacionados à Segurança da Informação; c) promover a capacitação dos recursos humanos para o desenvolvimento de competência científico-tecnológica em Segurança da Informação.

O Projeto de Lei ora apresentado atribui à CODEPLAN a definição das diretrizes da Política de Segurança da Informação, coordenando e regulamentando as atividades inerentes.

Considerando a premência da matéria, solicito a Vossa Excelência que a presente proposta legislativa tramite em **regime de urgência.**

Na oportunidade, renovo a Vossa Excelência e seus ilustres pares protestos de estima e consideração.

Atenciosamente,

JOAQUIM DOMINGOS RORIZ
Governador do Distrito Federal

PL 3133 /2002

PROJETO DE LEI n'

(Do Poder Executivo)

Dispõe sobre a prevenção das entidades públicas do Distrito Federal com relação aos procedimentos praticados na área de informática e dá outras providências.

A Câmara Legislativa do Distrito Federal DECRETA:

CAPÍTULO I

Seção I

DOS PRINCÍPIOS

Art. 1º Esta lei estabelece normas gerais sobre a prevenção das entidades públicas do Distrito Federal com relação aos procedimentos praticados na área de informática.

Parágrafo único – Subordinam-se ao regime desta lei, alem dos órgãos da Administração Direta, as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pelo Governo do Distrito Federal.

Seção II

DOS PRINCÍPIOS QUE REGEM A SEGURANÇA DA INFORMAÇÃO

Art. 2º As entidades públicas do Distrito Federal devem formular estratégias e adotar mecanismos que assegurem suas informações em relação aos aspectos de disponibilidade, integridade, confidencialidade e autenticidade.

§ 1º Para fins desta Lei, entende-se por estratégias as políticas, diretrizes e ações voltadas para a implementação de requisitos de Segurança da Informação nos processos institucionais;

§ 2º As estratégias devem estar em consonância com as legislações vigentes, de forma a evitar violações de natureza civil ou criminal.

Art. 3º A estratégia de Segurança da Informação deve prever a adoção de mecanismos de controle preventivos e corretivos, abrangendo princípios de segurança física e lógica.

CAPÍTULO II

DOS PRINCÍPIOS DE PROTEÇÃO PREVENTIVA DA INFORMAÇÃO

Seção I

DA SEGURANÇA FÍSICA

Art. 4º A proteção física dos equipamentos de informática, telecomunicações e outros equipamentos técnicos do gênero deve ser assegurada mediante o acondicionamento em ambientes ou compartimentos adequados, providos de mecanismos de controle de acesso.

Seção II

DA SEGURANÇA LÓGICA

Art. 5º A proteção lógica dos serviços de informática deve ser assegurada mediante identificação e autenticação dos usuários, respeitando-se os direitos de privacidade e segurança.

Seção III

DA PROTEÇÃO DE DADOS E PROGRAMAS

Art. 6º Os programas de computador devem assegurar a integridade e a confidencialidade das informações processadas e armazenadas em bases de dados.

Parágrafo único - O mecanismo de proteção das bases de dados deve restringir a leitura, criação, modificação, gravação, recepção e exclusão de registros apenas a usuários autorizados.

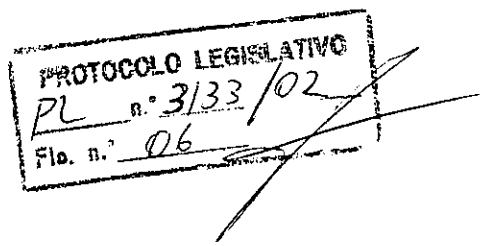
CAPÍTULO III

DOS PRINCÍPIOS DE PROTEÇÃO CORRETIVA DA INFORMAÇÃO

Art. 7º Os ambientes informatizados devem estar dotados de mecanismos e procedimentos que assegurem a continuidade dos serviços classificados como críticos pela Administração.

CAPÍTULO IV

DOS COMPORTAMENTOS IRREGULARES



Art. 8º São considerados comportamentos irregulares:

I - Negligenciar os cuidados relativos ao armazenamento, manuseio e descarte das informações que lhe foram confiadas, independentemente do meio utilizado.

II - Apagar, destruir, modificar ou inutilizar, total ou parcialmente, de forma indevida ou não autorizada, dados ou programas de computador.

III - Obter, manter ou fornecer a terceiros, de forma indevida ou não autorizada, acesso a computadores ou à rede de computadores, dados ou informações.

IV - Criar, desenvolver ou inserir dado ou programa em computador ou rede de computadores com a finalidade de apagar, destruir ou modificar dado ou programa, dificultando ou impossibilitando, total ou parcialmente, sua utilização.

V - Disseminar serviço ou informação de caráter pornográfico ou discriminatório em rede de computadores.

VI - Outros comportamentos definidos pela Administração.

CAPÍTULO V

DAS PENALIDADES

Art. 9º Os comportamentos discriminados no artigo anterior desta Lei serão apurados na forma da legislação vigente, quando praticados:

I – com prejuízo financeiro para a entidade;

II – com intuito de lucro ou vantagem de qualquer espécie, em benefício próprio ou de terceiros;

III – por meio de falsificação de identidade;

IV – de forma que denigra a imagem da entidade;

V – com a utilização de meios fraudulentos.

Art. 10. Serão aplicadas as sanções dispostas na legislação vigente, àqueles que adotarem os comportamentos definidos no Capítulo IV da presente Lei.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

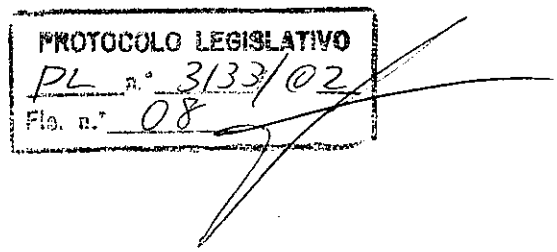
Art. 11. Esta Lei regula os procedimentos relativos à Segurança da Informação sem prejuízo das demais cominações previstas em outros diplomas legais.

Art. 12. Ficará a cargo da Companhia de Desenvolvimento do Planalto Central – CODEPLAN, empresa pública do Distrito Federal, a formulação das estratégias definidas nesta Lei.

Art. 13. O Poder Executivo regulamentará esta Lei no prazo de trinta dias.

Art. 14. Esta Lei entra em vigor na data de sua publicação.

Art. 15. Revogam-se as disposições em contrário e a Lei nº 2.572, de 20 de julho de 2000.



CÂMARA LEGISLATIVA DO DISTRITO FEDERAL
LEI Nº 2.572, DE 20 DE JULHO DE 2000

Dispõe sobre a prevenção das entidades públicas do Distrito Federal com relação aos procedimentos praticados na área de informática.

O GOVERNADOR DO DISTRITO FEDERAL, FAÇO SABER QUE A CÂMARA LEGISLATIVA DO DISTRITO FEDERAL DECRETA E EU SANCIONO A SEGUINTE LEI:

CAPÍTULO I

DOS PRINCÍPIOS QUE REGULAM AS CONDIÇÕES

DE SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO

E DE INFORMAÇÃO COMO FONTE DE DADOS

Art. 1° As entidades públicas do Distrito Federal devem promover a segurança da informação, mediante a garantia da disponibilidade, integridade, confiabilidade e legalidade das informações que suportam os seus processos operacionais.

Art. 2° A garantia da disponibilidade deve ser de forma preventiva e abranger os aspectos físicos, lógicos e técnicos.

CAPÍTULO II

DOS PRINCÍPIOS DA PROTEÇÃO

PREVENTIVA DA INFORMAÇÃO

Seção I

Da Segurança Física

Art. 3° A proteção física dos equipamentos, servidores de rede, telecomunicação e outros deve ser garantida mediante o acondicionamento em ambientes ou compartimentos e controle de acesso adequados.

Parágrafo único. Entende-se por ambiente adequado aquele que proteja os equipamentos críticos de informática e informações vitais segundo exigências mínimas de temperatura e umidade, ou seja, 20°C e 85% de umidade relativa do ar.

Seção II

Da Segurança Lógica

Art. 4° A proteção lógica dos sistemas deve ser garantida mediante a definição dos papéis dos usuários e das regras de acesso à informação, respeitados os critérios de garantia dos

direitos individuais e coletivos de privacidade e segurança de pessoas físicas e jurídicas.

Seção III

Da Proteção de Dados e Programas

Art. 5° Os padrões e soluções de segurança de dados de programas devem garantir a sua proteção quanto à disposição dos usuários, enquanto instalados nos servidores de arquivos, ou nas estações de nível de descrição no registro dos eventos e na preservação contra vírus de computadores.

§ 1° A proteção de dados e programas instalados no servidor de arquivos deve garantir padrões de segurança contra leitura, execução, gravação, recepção e criação por parte de pessoas não autorizadas.

§ 2° Qualquer pessoa, física ou jurídica, tem o direito de interpelar o proprietário de redes de computadores ou provedor de serviços para saber informações ao seu respeito e o respectivo teor.

Art. 6° O acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em rede de computadores dependerá de prévia autorização judicial.

CAPÍTULO III

DOS ASPECTOS DE RECUPERAÇÃO DA INFORMAÇÃO

Art. 7° O gerenciador e administrador de ambientes informatizados deve providenciar análise de risco físico e lógico, abrangendo padrões definidos para acondicionamento de equipamentos de processamento de dados e mídias magnéticas, e identificando possíveis prejuízos.

Art. 8° O administrador dos ambientes de tecnologia da informação deverá desenvolver plano de contingência.

Parágrafo único. Os planos de contingência devem conter as alternativas para os processos e as fases de pré-interrupção, interrupção e pós-interrupção.

CAPÍTULO IV

DOS COMPORTAMENTOS IRREGULARES

Seção I

Disposições Preliminares

Art. 9° Os comportamentos discriminados nos arts. 10 a 16 desta Lei serão apurados na forma estabelecida na Lei n° 8.112, de 11 de dezembro de 1990, quando praticados na forma abaixo:

I – com considerável prejuízo para a entidade;

II – com intuito de lucro ou vantagem de qualquer espécie, próprio ou de terceiros;

III – com abuso de confiança;

IV – por motivo fútil;

V – com o uso indevido de senha ou processo de identificação de terceiros;

VI – com a utilização de qualquer outro meio fraudulento.

Parágrafo único. Aplicar-se-á o disposto no *caput* quando os comportamentos se verificarem em órgãos ou entidades da administração direta ou indireta da União, dos Estados e do Distrito Federal, empresas concessionárias de serviços públicos, fundações instituídas ou mantidas pelo Poder Público, empresas de serviços sociais autônomos, instituições financeiras ou empresas que explorem ramo de atividade controlada pelo Poder Público, localizados no Distrito Federal.

Seção II

Da Negligência ou Omissão de Informações

Art. 10. Negligenciar ou omitir informações no tratamento, guarda e manuseio dos sistemas e redes de computadores e dados.

Seção III

Da Alteração de Dados

ou Programas de Computador

Art. 11. Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dados ou programas de computador, de forma indevida ou não autorizada.

Seção IV

Do Acesso ou da Obtenção Indevidos ou Não Autorizados de Dados ou Instrução de Computador

Art. 12. Obter acesso, manter ou fornecer a terceiro, dados, instrução ou qualquer meio de identificação ou acesso a computador ou a rede de computadores, de forma indevida ou não autorizada.

Seção V

Da Alteração de Senha ou Mecanismo de

Acesso a Programa de Computador ou Dados

Art. 13. Apagar, destruir, alterar ou de qualquer forma inutilizar senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada.

Seção VI

Da Violação de Segredos Armazenados

em Computador, Meio Eletrônico de Natureza Magnética, Óptica ou Similar

Art. 14. Obter segredos das entidades de que trata esta Lei, da indústria ou do comércio, ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada.

Seção VII

Da Criação, do Desenvolvimento e

da Inserção em Computador de Dados ou Programa de Computador com Fins Nocivos

Art. 15. Criar, desenvolver ou inserir dados ou programa em computador ou rede de computadores, de forma indevida ou não autorizada, com a finalidade de apagar, destruir, inutilizar ou modificar dados ou programa de computador, ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores.

Seção VIII

Da Veiculação de Pornografia

por Meio de Rede de Computadores

Art. 16. Disseminar serviço ou informação de caráter pornográfico em rede de computadores, sem exibir previamente, de forma facilmente visível e destacada, aviso sobre a sua natureza, indicando o seu conteúdo.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Art. 17. Serão aplicadas as sanções dispostas na Lei n° 8.112, de 11 de dezembro de 1990, àqueles que adotarem os comportamentos definidos na presente Lei.

Art. 18. Esta Lei regula os procedimentos relativos a informática sem prejuízo das demais cominações previstas em outros diplomas legais.

Art. 19. O Poder Executivo regulamentará esta Lei no prazo de trinta dias.

Art. 20. Esta Lei entra em vigor na data de sua publicação.

Art. 21. Revogam-se as disposições em contrário.

Publicada no DODF de 21.07.2000.