SERVIÇO PÚBLICO FEDERAL
INSTITUTO NACIONAL DE TECNOLOGIA

Portaria nº 010, de 29 de janeiro de 2010

O DIRETOR DO INSTITUTO NACIONAL DE TECNOLOGIA, no uso das atribuições que lhe foram conferidas por Delegação de Competência, constante da Portaria nº 407, de 29.06.2006, publicada no D.O.U. de 30.06.2006 e, pelo Regimento Interno do INT, aprovado pela Portaria MCT nº 201, de 24.03.2009, publicada no D.O.U. de 26.03.2009, ambas assinadas pelo Senhor Ministro de Estado da Ciência e Tecnologia,

RESOLVE:

Art. 1º – Aprovar a Política de Utilização dos Recursos Computacionais, que define as Diretrizes para Utilização dos Recursos Computacionais e a Segurança da Informação, visando preservar a integridade, confidencialidade e disponibilidade das informações sob a gestão do INT, na forma do anexo à presente Portaria.

Art. 2º – Esta Portaria entra em vigor na data de sua assinatura, devendo ser publicada no Boletim de Pessoal.

Domingos Manfredi Naveiro
Diretor

INSTITUTO NACIONAL DE TECNOLOGIA
MINISTÉRIO DA CIÊNCIA E TECNOLOGIA

POLÍTICA DE UTILIZAÇÃO DOS
RECURSOS COMPUTACIONAIS

Divisão de Informática – DINF
Rio de Janeiro, 2009

APRESENTAÇÃO

Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples. Bastava trancar os documentos em um lugar e restringir o acesso físico àquele local. Com as mudanças tecnológicas e o uso de computadores de grande porte, a estrutura de segurança já ficou um pouco mais sofisticada, englobando controles lógicos, porém ainda centralizados. Com a chegada dos computadores pessoais e das redes de computadores que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes e métodos de segurança cada vez mais sofisticados. Paralelamente, os sistemas de informação também adquiriram importância vital para a sobrevivência da maioria das organizações modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação torna-se inviável.

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades.

A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, trasmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio (ABNT NBR ISO/IEC 17799:2005).

De acordo com o RFC 2196 (*The Site Security Handbook*), uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização.

O Instituto Nacional de Tecnologia – INT, ciente da importância de seu papel inovador e tecnológico perante a Administração Pública Federal e a Sociedade Brasileira, elaborou esta política de utilização dos recursos computacionais com o intuito de estabelecer diretrizes e princípios gerais para implementar, manter e melhorar a gestão de segurança da informação.

COMPOSIÇÃO DA DIREÇÃO DO INT

Diretoria – DIR
Diretor: Domingos Manfredi Naveiro
Substituto: Carlos Alberto Marques Teixeira

Coordenação Geral Regional do Rio de Janeiro – CGRJ
Coordenador: Lygia Vilmar Britto
Substituto: Maria Marta Gomes de Souza

Coordenação de Gestão de Contratos e Convênios – COGC
Coordenador: Haroldo de Jesus Clarim
Substituto: Maria Gabriela Pinto de Almeida Simões

Coordenação de Articulação e Representação Institucional – COAR
Coordenador: Andrea Lessa da Silva Costa
Substituto: Jorge Pereira da Silva

Coordenação de Desenvolvimento Tecnológico – CODT
Coordenador: Paulo Gustavo Pries de Oliveira
Substituto: Alexandre Barros Gaspar

Coordenação de Tecnologias Aplicadas – COTA
Coordenador: Attilio Travalloni
Substituto: Ieda Maria Vieira Caminha

Coordenação de Engenharia – COEN
Coordenador: Ieda Maria Vieira Caminha
Substituto: Valeria Said de Barros Pimentel

Coordenação de Gestão da Qualidade e Inovação Tecnológica – COQI
Coordenador: Carlos Alberto Marques Teixeira
Substituto: Telma de Oliveira

Coordenação de Logística e Infra-estrutura – COIN
Coordenador: Ivan Magalhães Pereira
Substituto: Márcio Leocádio de Sant'Anna

Equipe de Desenvolvimento – DINF
Supervisão: Ricardo Ferreira Vieira de Castro
Elaborado por: Luiz Fernando da Silva Dias
Apoio: Carolina Schutt Torrescasana
Érico Travassos Lemos
José Vitor Cruz de Souza
Vinicius Silva Vieira

SUMÁRIO

1 INTRODUÇÃO

1.1 Aplicação

1.1.1 Esta Política define as Diretrizes para Utilização dos Recursos Computacionais e a Segurança da Informação, visando preservar a integridade, confidencialidade e disponibilidade das informações sob gestão do INT. Descreve a conduta considerada adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentalmente ou intencionalmente.

1.1.2 Esta Política aplica-se a todos os funcionários e colaboradores do **Instituto Nacional de Tecnologia - INT** que utilizam os recursos computacionais da **REDE DE COMPUTADORES DO INT.**

1.2 Considerações Iniciais

1.2.1 Esta Política deve ser conhecida e obedecida por todos os usuários que utilizam os recursos de processamento da informação de propriedade ou controlados pelo INT, sendo de responsabilidade de cada um o seu cumprimento. A Política está disponível na intranet do INT (http://intranet.int.gov.br).

1.2.2 Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas pelos usuários, quando da utilização dos recursos de processamento da informação no INT, ficando os transgressores sujeitos às sanções previstas nestas diretrizes.

1.2.3 A **Divisão de Informática – DINF** é a responsável pela gestão dos sistemas de informação e dos recursos computacionais de processamento, transmissão de dados e informações.

1.2.4 São definidos como recursos computacionais todos os elementos lógicos e físicos responsáveis pelo armazenamento, transmissão, captura, processamento e publicação de dados, contemplando também elementos de infra-estrutura, dados e informação por eles contidos ou trafegados.

1.2.5 Todo e qualquer uso de recursos computacionais do **INT** deve estar de acordo com as obrigações legais assumidas, inclusive com as limitações definidas nos Contratos de programas de computador (*software*) e outras licenças.

1.2.6 Em caso de mau funcionamento do equipamento de informática, o usuário deverá solicitar suporte técnico à **DINF**, através do **Sistema de Suporte à Informática - SSI** (disponível na *Intranet*).

1.2.7 As solicitações de suporte técnico somente serão atendidas quando efetuadas através da **SSI**.

1.2.8 Não é permitido o uso de material de consumo de informática do **INT** para fins particulares.

1.2.9 A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais previstas no Regime Único dos Servidores Públicos (Lei nº 8.112/90, Título IV (Capítulos I, II, IV e V) e Título V (Capítulos I, II e III)), no Código Penal (Decreto-Lei Nº 2.848/40, com as alterações da Lei Nº 9.983/00 e no Decreto N° 2.910/98), no Novo Código Civil (Lei 10.406 de 10/01/2002) ou em qualquer outra legislação que regule ou venha regular a matéria.

1.2.10 As empresas incubadas ficarão em uma rede separada da rede administrativa do INT, tendo, somente, acesso a internet.

1.2.11 A Internet e o correio eletrônico, no âmbito do INT, são uma concessão e não um direito. Portanto, sua utilização, deve ser exclusivamente para atividades ligadas ao trabalho da Instituição;

1.2.12 Será de responsabilidade de cada usuário zelar pelo fiel cumprimento ao estabelecido na presente Norma, devendo o usuário tomar ciência e assinar o “Termo Individual de Responsabilidade” anexado à mesma.

2 NORMAS DE CONTAS E SENHAS PARA USUÁRIOS

2.1 Objetivo

Definir procedimentos e responsabilidades para cadastramento de usuários e para acesso à rede de computadores do INT.

2.2 Conceito

2.2.1 Segundo a norma ABNT NBR ISO/IEC 17799:2005, item 11.2, procedimentos formais devem ser implementados para controlar a distribuição do direito de acesso a sistemas de informação e serviços. Orienta ainda que a concessão e o uso de privilégios sejam restritos e controlados (item 11.2.2) e que a concessão de senhas seja controlada através de um processo de gerenciamento formal (item 11.2.3).

2.2.2 Deste modo, o INT elaborou esta norma de contas e senhas para usuários, de forma a zelar pelo uso apropriado de senhas, que pode vir a ser um grande inibidor de falhas ou violações de sistemas e informações.

2.3 Cadastro de Usuários

2.3.1 Para utilizar qualquer recurso computacional do INT, é necessário que o usuário esteja cadastrado na REDE DE COMPUTADORES DO INT. As empresas incubadas como não fazem parte da rede lógica do INT, só terão acesso a internet.

2.3.2 Para que o usuário seja cadastrado é necessário o preenchimento do Formulário de Criação de Usuários disponível na intranet (http://intranet.int.gov.br).

2.3.3 O preenchimento do Formulário para SERVIDORES, ESTAGIÁRIOS, BOLSISTAS e PRESTADORES DE SERVIÇO, deverá ser realizado pelas divisões/coordenações e encaminhados á Divisão de Recursos Humanos – DARH.

2.3.3.1 No formulário deverá constar, nos casos de Bolsistas, Estagiários e Prestadores de Serviço, o período de validade do cadastramento.

2.3.4 Ficará sob responsabilidade da DINF informar ao usuário sobre a efetivação de seu cadastramento na REDE DE COMPUTADORES DO INT, informando também a senha padrão e a identificação do usuário (*login*) para efetuar a primeira conexão.

2.3.5 Alterações de dados dos usuários da rede do INT deverão ser solicitadas pela Divisão de Recursos Humanos, encaminhando as informações necessárias através da SSI.

2.3.6 Bloqueio de Usuários:

2.3.6.1 No caso de Bolsistas, Estagiários e Prestadores de Serviços, ao fim do prazo de validade do cadastramento, a conta será bloqueada automaticamente. Para bloqueio antes do término do prazo, o mesmo deverá ser solicitado pela chefia imediata do usuário;

2.3.6.2 No caso de Servidores, o bloqueio deverá ser solicitado pela chefia imediata através da Divisão de Recursos Humanos.

2.3.7 A exclusão da conta do usuário (Servidor) só será efetuada mediante apresentação do Formulário de Pesquisa de Débito de Pessoal devidamente preenchido, no caso de Prestadores de Serviço, Estagiários e Bolsistas, a conta será excluída mediante solicitação do DARH.

2.4 *Login* e Senha de Usuários

2.4.1 Quando efetuada a primeira conexão, o usuário deverá alterar a senha padrão por uma de sua escolha, conforme descrito no item 2.4.3.

2.4.2 O *login* é definido pelo usuário com base no seu nome e um sobrenome. Não serão permitidos apelidos ou codinome. *Ex.: Moysés da Silva Pires → moyses.silva* ou *moyses.pires*.

2.4.3 A senha e o *login* são pessoais, intransferíveis e de inteira responsabilidade do usuário.

2.4.3.1 As senhas não poderão possuir tamanho inferior a 6 (seis) caracteres e superior a 14 (quatorze) caracteres.

2.4.3.2 Recomenda-se que as senhas sejam mescladas com letras do alfabeto (maiúscula e minúscula), números e caracteres especiais que não tenham qualquer vínculo lógico com o usuário.

2.4.3.3 Recomenda-se ao usuário evitar escolher como senha o seu próprio *login*, combinações do nome do usuário, datas, telefones, placas de carro, endereços, nome dos filhos ou outros de fácil assimilação.

2.4.3.4 Para maior segurança sugere-se que o usuário realize a troca de sua senha, no máximo, a cada 6 (seis) meses.

2.4.3.5 Quando ocorrer mais de 3 (três) tentativas de acesso inválidas, o *login* do usuário será bloqueado, sendo necessário solicitar o desbloqueio à DINF.

2.4.3.6 Caso o usuário suspeite do comprometimento de sua senha, a mesma deverá ser modificada imediatamente.

2.4.4 Não é permitido ao usuário ceder, mesmo que temporariamente, seu *login* e senha da Rede do INT para utilização por outras pessoas, sejam estas integrantes do quadro de servidores/colaboradores do INT ou não, ficando o cedente responsável pelos atos praticados indevidamente com a mesma.

2.4.5 O usuário deve bloquear sua estação de trabalho ou efetuar o encerramento da seção (*logoff*) sempre que se ausentar do seu local de trabalho e desligá-la sempre que terminar sua jornada de trabalho.

2.4.6 O *login* que ficar inativo por mais de 50 (cinquenta) dias irá ser bloqueado automaticamente.

2.4.7 Em caso de aposentadoria do usuário, a conta será bloqueada automaticamente por um prazo de 30 dias. Durante este período uma mensagem de resposta automática estará disponível em seu email. Após esse prazo, a conta será excluída.

2.5 Disposições Gerais

2.5.1 Todos os usuários terão conta com perfil padrão, ou seja, são impedidos de fazer alterações acidentais ou intencionais no âmbito do sistema. Podem executar aplicativos certificados, mas não podem instalar programas e nem desinstalar os que já estão instalados;

2.5.2 Os usuários somente poderão requerer conta com perfil administrativo caso esteja utilizando regularmente algum programa que exija a utilização deste perfil. A solicitação deverá ser feita por escrito com as devidas justificativas técnicas. A alteração de perfil deverá ter a concordância da chefia imediata;

2.5.3 Os usuários somente poderão requerer conta com perfil avançado caso suas atividades necessitem a constante instalação de programas. A solicitação deverá ser feita por escrito com as devidas justificativas técnicas. A alteração de perfil deverá ter a concordância da chefia imediata;

2.5.4 A eventual necessidade de instalação de softwares deve ser solicitada via SSI, à Divisão de Informática – DINF, de forma haver um controle centralizado de softwares e licenças disponíveis para o INT.

3 CORREIO ELETRÔNICO

3.1 Objetivo

Prover a comunicação é, sem dúvida, a essência das redes. As pessoas sempre procuraram se corresponder da maneira mais rápida e fácil possível. O correio eletrônico (e-mail) é a aplicação que mais ilustra esta procura. A facilidade de correio eletrônico fornecido pelo INT deve ser usada no interesse do serviço.

3.2 Responsabilidades

3.2.1 Cabe a **DINF:**

3.2.1.1 Garantir a disponibilidade do Serviço de Correio Eletrônico em níveis adequados à necessidade do trabalho.

3.2.1.2 Manter processo sistemático de gravação e retenção de arquivos de registro (logs) de mensagens de correio eletrônico. Os arquivos de registro serão mantidos por 6 (seis) meses.

3.2.1.3 Em caso de notificação judicial, administrativa ou de auditoria, será suspensa a eliminação dos arquivos de registros e do conteúdo das caixas de Correios Eletrônico.

3.2.1.4 Manter a integridade e a disponibilidade do Serviço de Correio Eletrônico, no âmbito do INT.

3.2.2 Cabe ao **usuário:**

3.2.2.1 Utilizar o Correio Eletrônico institucional para os objetivos e funções próprios e inerentes às suas atribuições funcionais;

3.2.2.2 Eliminar, de preferência diariamente, as mensagens contidas nas caixas de Correio Eletrônico, evitando assim o descarte automático de mensagens recebidas;

3.2.2.3 Não permitir acesso voluntário de terceiros a sua conta de Correio Eletrônico;

3.3 Utilização

3.3.1 O Serviço de Correio Eletrônico é uma ferramenta de trabalho.

3.3.2 O acesso ao Correio Eletrônico se dá pelo conjunto Identificação do Usuário e Senha.

3.3.3 Aos usuários somente será permitido possuir caixa de Correio Eletrônico do INT para uso nas atividades relacionadas ao trabalho desempenhado na Instituição.

3.3.4 Sobre a propriedade e o direito de uso do Serviço de Correio Eletrônico do INT fica definido que:

3.3.4.1 As caixas do Correio Eletrônico são de propriedade do INT com concessão de uso aos usuários;

3.3.4.2 Será assegurado pela DINF, a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na lei nº 9.296/96 e no inciso XII do artigo 5º da Constituição Federal;

3.3.4.3 A DINF, dentro da garantia de inviolabilidade da privacidade do usuário, reserva-se ao direito de monitorar o uso do Correio Eletrônico, podendo ainda exercer fiscalização com fins de auditoria nos casos de apuração de uso indevido desse recurso quando autorizado pela direção da Instituição.

3.3.5 O tamanho das mensagens (texto mais arquivos anexados) é limitado, tanto para envio quanto para recebimento em 20 Mb (vinte *megabytes*).

3.3.6 O tamanho de armazenagem de dados das caixas de Correio Eletrônico é definido pela DINF, bem como as permissões para acesso às caixas de Correio Eletrônico. Inicialmente, cada conta de Correio Eletrônico possui uma capacidade de 500 Mb (quinhentos *megabytes*).

3.3.7 É permitido, ao usuário, o envio de mensagens com até 30 (trinta) destinatários, internos ou externos;

3.3.7.1 Os usuários que, no interesse do trabalho, necessitarem enviar mensagens com número maior de destinatários, devem solicitar esta facilidade à DINF, justificando sua necessidade.

3.3.8 Podem ser criadas listas de distribuição no Servidor de Correio Eletrônico visando facilitar o envio de mensagens para grupos de destinatários pré-estabelecidos.

3.3.8.1 A criação e a manutenção das listas de distribuição é de responsabilidade da DINF.

3.3.8.2 As listas de distribuição somente serão criadas mediante solicitação dos representantes das Unidades junto à DINF através da SSI.

3.3.8.3 As listas existentes bem como suas características estão disponíveis na intranet (http://intranet.int.gov.br).

3.3.8.4 Toda solicitação de lista deverá ser aprovada pela direção do INT.

3.3.9 Não é permitida tentativa de acesso não autorizado às contas de Correio Eletrônico de terceiros, bem como o envio de informações confidenciais do INT, para pessoas ou organizações não autorizadas.

3.3.10 Contas de email com inatividade por um período igual ou superior a 50 (cinquenta) dias serão bloqueadas. Esta regra não se aplica as contas vinculadas aos cargos/funções (p.ex. dinf@int.gov.br), por serem inerentes as atribuições desses cargos/funções.

3.3.11 Em caso de desligamento do usuário, o chefe imediato deverá informar a DARH para que solicite junto à DINF, a exclusão da caixa de Correio Eletrônico, ressalvado o disposto subitem 3.2.1.3.

3.3.12 Para recuperar e trabalhar com o e-mail em casa ou em outro local que tenha acesso à *Internet*, o usuário deve utilizar o *webmail* do INT (https://mail.int.gov.br/owa).

3.3.12.1 Apenas as mensagens que estão no Servidor de Correio Eletrônico, podem ser acessadas via *webmail* do INT, ou seja, se os e-mails estiverem em pastas locais os mesmos estarão inacessíveis.

3.3.12.2 Após o término da utilização do *webmail* do INT, deve ser efetuado *logoff*, para que a sessão entre o cliente e o Servidor de Correio Eletrônico seja fechada.

3.3.13 Aplicam-se ao Correio Eletrônico as Normas de Classificação de Informações vigentes na Administração Pública Federal, conforme legislação em vigor.

3.4 **Restrições**

3.4.1 Para efeito de envio, recebimento e armazenamento de mensagens não serão permitidos:

3.4.1.1 A promoção de negócios particulares tais como comércios, propagandas e afins;

3.4.1.2 O envio de:

3.4.1.2.1 de material obsceno, ilegal ou não ético, comercial pessoal, mensagens do tipo corrente, entretenimento e mensagens não solicitadas a um grande número de pessoas (*spam*);

3.4.1.2.2 de mensagens que sejam ofensivas podendo causar tormento ou ainda afetar de forma negativa a imagem do Instituto Nacional de Tecnologia – INT;

3.4.1.2.3 de mensagens contendo vírus de computador ou qualquer forma de rotinas de programação prejudiciais ou danosas;

3.4.1.3 O recebimento de:

3.4.1.3.1 músicas, vídeos, e qualquer arquivo binário executável (exe, com, bat, scr, etc...);

3.4.1.4 O envio das listas de endereços eletrônicos dos usuários do Correio Eletrônico do INT;

3.4.1.5 O tráfego de material protegido por leis de propriedade intelectual.

3.5 **Recomendações**

3.5.1 Para o bom uso do Serviço de Correio Eletrônico:

3.5.1.1 O remetente deve, além de se identificar de forma clara e evidente em todas as suas mensagens de Correio Eletrônico, redigir as mensagens de forma clara e sucinta, mantendo o grau de formalidade compatível com o destinatário e o assunto;

3.5.1.2 Não devem ser abertos arquivos anexo a mensagens de procedência desconhecida, principalmente quando forem arquivos executáveis;

3.5.1.3 Os arquivos anexados às mensagens devem ser salvos em disco e verificados com o programa de antivírus, antes de serem abertos;

3.5.1.4 Os arquivos que forem anexados às mensagens a serem enviadas, devem ser verificados com o programa de antivírus;

3.5.1.5 Quando alguma mensagem retornar a caixa postal do usuário por problemas de entrega, deve ser verificado se o endereço do destinatário está correto ou se a mensagem não excede o tamanho máximo permitido para envio (20 MB - vinte *megabytes*). A mensagem de retorno enviada pelo Servidor de Correio Eletrônico deve ser lida com atenção. No caso de não entendê-la, o usuário deve entrar em contato com a DINF para esclarecimentos e posterior reenvio da mensagem.

3.6 **Disposições finais**

3.6.1 O uso indevido dos serviços de correio eletrônico, tratados neste documento, é passível de sanção disciplinar, de acordo com a legislação vigente e demais Normas aplicadas à matéria.

3.6.2 O servidor, no ato da publicação de sua aposentadoria, terá sua conta de email bloqueada por 30 dias. Neste período, será incluída no seu email uma mensagem de auto-resposta informando que o mesmo já não faz parte do corpo funcional do INT, passado este período a conta será cancelada.

3.6.3 O servidor que estiver em licença sem vencimento, terá sua conta de email bloqueada por um período indeterminado. Será incluída no seu email uma mensagem de auto-resposta informando que o mesmo está ausente sem data de retorno.

3.6.4 Em caso de licença prêmio ou férias, o servidor não terá alterações na sua conta de email, de modo que o serviço de auto-resposta é opcional e configurado pelo usuário.

4 SEGURANÇA

4.1 Objetivo

Definir responsabilidades e procedimentos que garantam a confidencialidade, a integridade e a disponibilidade das informações e serviços da REDE DO INT.

4.2 Responsabilidades

4.2.1 Cabe à **DINF**:

4.2.1.1 Administrar com segurança as informações disponíveis no ambiente de TI do INT.

4.2.1.2 Implementar e manter mecanismos de segurança.

4.2.1.3 Fazer cópias de segurança (*backup*) dos dados contidos nos Equipamentos Servidores de Rede, que guardará um histórico mínimo de 6 (seis) meses. Somente serão objetos de *backup*, dados e informações relacionados às atividades desenvolvidas ou trabalhadas no âmbito interno do INT.

4.2.1.4 Os dados contidos na estação de trabalho do usuário não são de responsabilidade da DINF, estando o usuário responsável pelo backup local.

4.2.1.5 Identificar e documentar qualquer violação de acesso ou tentativas de violação.

4.2.1.6 Realizar auditoria periódica nos arquivos contidos nos Equipamentos Servidores de Rede do INT, uma vez que são de propriedade do Instituto, estando sob concessão de uso.

4.2.1.7 Monitorar a integridade das informações contidas nos Sistemas pertencentes ao INT.

4.2.1.8 Gerenciar acessos a arquivos, definindo seu grau de confidencialidade.

4.2.1.9 Garantir a integridade dos dados que trafegam no ambiente da REDE DO INT.

4.2.1.10 Manter controle de acesso para toda conexão entre a rede interna e a Rede Mundial de Computadores (*Internet*).

4.2.1.11 Definir, implementar e manter políticas de utilização das estações de trabalho, que possibilitem um melhor gerenciamento e uma melhor produtividade em todo ambiente de TI do INT, levando em consideração a segurança e a funcionalidade da REDE DO INT.

4.2.2 Cabe aos **Usuários**:

4.2.2.1 A realização de *backup*, dos dados contidos nas estações de trabalho.

4.2.2.1.1 Caso necessite do apoio da DINF para a realização do *backup* destes dados, o usuário deverá solicitá-lo através da SSI, disponível na *Intranet*.

4.2.2.1.2 O usuário deverá disponibilizar a mídia (CD ou equivalente) para realização do *backup*.

4.2.2.2 Manter sigilo absoluto, sobre os dados, informações e processos disponíveis no ambiente de TI do INT, que podem ser acessados através da utilização do seu *login* e senha.

4.3 Antivírus

4.3.1 O INT fornecerá e definirá qual o sistema de antivírus será utilizado pelas estações de trabalho e servidores de rede do INT;

4.3.2 A REDE DO INT está protegida por antivírus que monitora e realiza varreduras constantes para detecção e eliminação de vírus de computador no Servidor de Correio, nos Servidores de Dados e nas estações de trabalho, mas, é imprescindível que o antivírus seja sempre utilizado em situações como: recebimento de *e-mail* com arquivo anexado, ao fazer uma transferência de arquivo proveniente da Internet (*download*) ou trazer uma mídia de fora do ambiente do INT;

4.3.3 Os equipamentos que não fazem parte do parque tecnológico do INT não serão contemplados pelo sistema de antivírus.

4.4 Restrições

4.4.1 Não será permitido ao usuário utilizar a sua estação de trabalho para obter acesso não autorizado a qualquer outro recurso da REDE DO INT ou de outra rede remota.

4.4.2 Não será permitida a realização ou tentativa de acesso a dados ou estações de trabalho sem prévia autorização por parte de seu detentor ou responsável.

4.4.3 Não serão permitidos o acesso, utilização, instalação, manutenção e implementação de qualquer recurso computacional sem prévio conhecimento e autorização por parte da DINF.

4.4.4 Caso necessite de qualquer um dos serviços descritos no item 4.4.3, o usuário deverá solicitá-los através da SSI.

4.5 Acesso às Dependências

4.5.1 O acesso físico a qualquer dependência do prédio do INT, onde se encontram os equipamentos ativos da REDE DO INT, é restrito aos técnicos da DINF.

Exemplos*:* Sala dos Equipamentos Servidores de Rede, bastidores dos elementos ativos de rede, depósitos de informática, sala dos estabilizadores e qualquer outro tipo de dependência sob o controle da DINF.

4.5.2 O acesso de pessoas estranhas às dependências somente se dará com a devida autorização ou acompanhamento de pessoa devidamente credenciada pela DINF.

4.6 Observações

4.6.1 O INT não se responsabilizará por fraudes ocorridas em transações financeiras ou similares feitas na Internet decorrentes de mau uso ou agentes externos. Portanto, recomenda-se a utilização de recursos computacionais do próprio usuário e fora do ambiente de TI do INT o acesso a contas bancárias tipo internet banking e similares.

5 INTRANET E INTERNET

5.1 Objetivo

Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os usuários devem estar cientes, portanto, da peculiaridade da navegação na Internet, antes de acessá-la e de utilizar seus recursos.

Considerando que o uso da INTERNET, no âmbito do INT, é uma concessão e não um direito, é de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada desse importante recurso tecnológico.

5.2 Responsabilidades

5.2.1 Cabe à **DINF**:

5.2.1.1 manter a infra-estrutura de *hardware* e *softwares* necessárias à viabilização de acesso aos serviços da *Internet* e da *Intranet*;

5.2.1.2 elaborar, manter e gerenciar os *sites* hospedados no INT, considerando aspectos de adequação ao perfil da instituição, clareza e organização das informações;

5.2.1.3 Elaboração e manutenção do *site* da *Intranet* do INT devem seguir os seguintes critérios:

5.2.1.3.1 os serviços oferecidos aos usuários da rede do INT devem ser apresentados de forma clara e objetiva;

5.2.1.3.2 o *site* deve conter assuntos de interesse dos usuários, desde de que sejam observados aspectos de confidencialidade e oportunidade;

5.2.1.3.3 o *site* deve manter as bases de dados atualizadas e confiáveis, promovendo conteúdo de qualidade com atualização constante.

5.2.1.4 avaliar a transparência quanto ao uso das funcionalidades e quanto ao gerenciamento de arquivos e documentos;

5.2.1.5 avaliar a conformidade da *Intranet* com padrões e metodologia de desenvolvimento adotada, validação de códigos e métodos;

5.2.1.6 monitorar e controlar a ocorrência de erros com eficiência, bem como promover sua adequada correção.

5.3 Normas para a utilização da INTERNET

5.3.1 Não é permitida a utilização de *software* de *peer-to-peer* (P2P), tais como Napster, Kazaa, Emule e afins;

5.3.2 Não é permitido o acesso a sites de relacionamento, tais como Orkut, Gazzag e afins;

5.3.3 Não é permitido o acesso a sites de Proxy externo. As tentativas de acesso serão registradas e encaminhadas via email para o usuário com cópia para a chefia imediata;

5.3.4 Não é permitido acessar, armazenar ou transferir informações de conteúdo pornográfico, erótico, indecente, ofensivo ou que incentivem a violência ou a discriminação de raça ou credo;

5.3.5 A liberação de mensageiros instantâneos via *Internet* (ex: ICQ, MSN) ficará sob responsabilidade do chefe de cada divisão/coordenação, devendo este comunicar a DINF através da SSI;

5.3.6 A DINF possui mecanismos de autenticação, que determinam a titularidade de todos os acessos à Internet feitos por seus usuários;

5.3.7 É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas em listas de discussão;

5.3.8 Usuários com acesso à Internet não podem efetuar upload de qualquer software licenciado ao INT ou de dados de propriedade do INT e/ou de seus clientes sem a autorização expressa da Diretoria ou do responsável pelo software/dado;

5.3.9 A Internet, no âmbito do INT, é uma concessão e não um direito. Portanto, sua utilização, deve ser exclusivamente para atividades ligadas ao trabalho da Instituição;

5.3.10 O usuário deve utilizar a Internet de forma adequada e diligente;

5.3.11 O usuário deve utilizar a Internet observando a conformidade com a lei, a moral, os bons costumes aceitos e a ordem pública;

5.3.12 O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso;

5.3.13 É vedada a utilização de qualquer tipo de modem (Telefônico, ADSL, GPRS) em máquinas que estejam conectadas ao ambiente da Rede do INT. Caso seja identificado, a estação será bloqueada e a chefia imediata será comunicada;

5.3.14 O INT monitora e bloqueia automaticamente sites de pornografia, pedofilia e outros contrários à lei. O acesso à esses sites é terminantemente proibido, mesmo que os mesmos não estejam sendo bloqueados no sistema de segurança. As tentativas de acesso serão registradas e encaminhadas via email para o usuário com cópia para a chefia imediata do usuário;

5.4 **Observações**

Devido o bloqueio de sites ser baseado em um sistema automatizado, algumas páginas poderão ser bloqueadas inadvertidamente. Caso seja bloqueado um site cujo conteúdo esteja de acordo com esta política, o usuário pode solicitar o desbloqueio através da SSI.

O fato de um site não estar bloqueado não significa que o mesmo possa ser acessado pelos usuários. Deverão ser observados todos os preceitos desta política, desde a proibição de acesso a sites contrários à lei ao uso excessivo da Internet para assuntos não relativos a trabalho no horário do expediente, por exemplo.

5.5 **Sanção especial**

Qualquer acesso a sites que tiverem conteúdo de pedofilia, racismo ou qualquer outro assunto contrário à lei que, eventualmente, não esteja bloqueado no sistema de proteção do INT, é terminantemente proibido. A violação deste item implica em encaminhamento do assunto primeiramente á coordenação do usuário e, não sendo esclarecido, com aceitação formal pela DINF e pela Direção do INT, abertura do pertinente processo administrativo e encaminhamento do assunto à autoridade policial no sentido de abertura de inquérito policial na Delegacia de Repressão a Crimes de Informática do Estado do Rio de Janeiro – DRCI (Decreto Nº 26.209, de 19 de abril de 2000).

6 ARMAZENAMENTO DOS DOCUMENTOS ELETRÔNICOS

6.1 Objetivo

Definir critérios para utilização da área de dados disponíveis nos Equipamentos Servidores de Rede e nas estações de trabalho dos usuários.

6.2 Responsabilidades

6.2.1 Cabe à **DINF**:

6.2.1.1 Definir, implementar e manter os diretórios utilizados para armazenamento de dados na Rede;

6.2.1.2 Disponibilizar os diretórios de dados nos equipamentos Servidores de Rede, de acordo com a estrutura organizacional do INT.

6.2.1.3 Definir a estrutura de drives de rede no servidor de arquivos (domint – "G:", comum – "I:" e home – "H:"):

6.2.1.3.1 Domint – "G:" → área destinada ao armazenamento de documentos comuns ao INT onde os usuários podem ler e executar os arquivos nela contido;

6.2.1.3.2 Comum – "I:" → área destinada ao armanezamento dos documentos da divisão do usuário onde toda a divisão tem acesso;

6.2.1.3.3 Home – "H:" → área destinada ao armazenamento dos documentos do usuário. Apenas o usuário poderá acessar esta área, podendo gravar, alterar e excluir os arquivos nela armazenados, não sendo permitida a guarda de material obsceno, ilegal ou não ético;

6.2.1.4 Definir, implementar e manter as cotas de armazenamento de dados nos equipamentos Servidores de Rede do INT:

6.2.1.4.1 Quota do drive "G:" → 50 Gb;

6.2.1.4.2 Quota do drive "H:" → 2 Gb;

6.2.1.4.3 Quota do drive "I:" → 20 Gb.

6.2.1.5 Fazer o backup dos dados contidos nos servidores como descrito no item 4.2.1.3 desta política;

6.2.2 Cabe ao **Usuário**:

6.2.2.1 Limpar os arquivos que não são mais úteis da estação de trabalho de modo a gerar mais espaço em disco, não sobrecarregando o sistema operacional.

6.3 Utilização

6.3.1 Não é permitido o armazenamento de arquivos do tipo: áudio e vídeo, salvo em casos especiais;

6.3.2 Não é permitido o armazenamento de materiais pornográficos, eróticos, arquivos contendo vírus, arquivos pessoais não ligados ao trabalho e softwares ilegais. Caso seja identificado, o usuário será informado para apagar os arquivos em até 2 dias. A não observância desta solicitação, sua conta será bloqueada e a chefia imediata será comunicada.

7 EQUIPAMENTOS DE INFORMÁTICA (*HARDWARES*)

7.1 Objetivo

Definir regras e responsabilidades na utilização de equipamentos eletrônicos e de informática, visando:

- aumentar os cuidados do usuário com os equipamentos do INT que são utilizados no desenvolvimento de suas atividades;
- obter maior durabilidade dos equipamentos eletrônicos e de informática;
- reduzir os dispêndios com manutenção dos equipamentos.

7.2 Responsabilidades

7.2.1 Cabe à **DINF**:

7.2.1.1 Manter a infra-estrutura de *hardware* necessária à viabilidade da execução de atividades relacionadas aos serviços;

7.2.1.2 Providenciar instalação, realocação e manutenção dos equipamentos de informática;

7.2.1.3 Identificar a necessidade de adquirir novas tecnologias e levantar o custo envolvido;

7.2.1.4 Elaborar especificações técnicas para aquisição de equipamentos e dispositivos para a infra-estrutura da rede do INT.

7.3 Utilização

7.3.1 Todas as estações de trabalho da rede do INT deverão estar dentro dos padrões de programas de computador (*software*s) e configurações adotadas pela DINF;

7.3.2 As chefias imediatas, juntamente com os usuários, são responsáveis pelas estações de trabalho por eles utilizadas, zelando pela sua conservação e integridade física;

7.3.3 A ocorrência de furto, extravio ou eventual defeito de equipamento decorrente de mau uso, por negligência ou por descumprimento dos procedimentos descritos neste Manual, ensejará em apuração de responsabilidade do agente público;

7.3.4 Os equipamentos destinados a empréstimo (*notebook*, projetor de vídeo, etc.) serão utilizados internamente e serão retirados mediante entrega à DINF do Formulário de Empréstimo de Equipamentos devidamente preenchido e assinado. Disponível na Intranet;

7.3.5 Qualquer problema, não previsto neste Manual, identificado pelo usuário no equipamento sob sua responsabilidade, deverá ser notificado imediatamente à DINF.

7.3.6 Notebook:

7.3.6.1 Notebooks de visitantes não poderão se conectar na rede lógica do INT, deverão utilizar a rede sem fio “visitantes” caso necessitem de utilizar a internet;

7.3.6.2 Notebook de visitantes deverão requerer senha para ter acesso à internet através da rede “visitantes”;

7.3.6.3 Qualquer usuário cadastrado na rede poderá, através da intranet, emitir senha com prazo de 24hs para o visitante.

7.3.6.4 Notebooks de propriedade do INT, quando utilizados fora da instituição, deverão ser logados através da conta “*usernote*” e quando utilizados na rede do INT deverão ser logados no ambiente CORP/ “*conta”*, onde o perfil deste usuário será carregado automaticamente com todas as definições de segurança previamente definidas.

7.3.7 Fica restrito à DINF proceder à abertura dos gabinetes das estações de trabalho do INT.

7.3.8 É expressamente proibida a instalação de equipamentos ou componentes para envio de fax ou conexão com redes externas (*Modem ou Fax/Modem*) em estações de trabalho que estejam conectados à rede do INT.

7.3.9 Qualquer equipamento, interno ou externo às estações de trabalho, que for ligado na rede do INT por área ou pessoa não autorizada, ou ainda, sem autorização expressa da DINF, será devidamente retirado e entregue ao proprietário ou recolhido à DINF, caso o proprietário não se encontre presente.

7.3.10 As solicitações de apoio para montagem de infra-estrutura de informática em eventos internos deverão ser encaminhadas à DINF com antecedência mínima de 10 (dez) dias úteis através da SSI.

7.4 **Desfazimento**

7.4.1 A área que necessitar desfazer de algum equipamento de informática deverá seguir as seguintes etapas:

7.4.1.1 Entrar em contato com a DINF, através da SSI, solicitando a avaliação do equipamento;

7.4.1.2 Caso o técnico constate que o equipamento não tem mais utilidade, a DINF deverá elaborar um memorando de análise técnica para a área requisitante atestando a inviabilidade do conserto ou a incapacitação do equipamento. Caso contrário, a DINF solicitará a transferência do equipamento (TRP);

7.4.1.3 Atestado a incapacidade do equipamento, á área solicitante deverá entrar em contato com a DSUP para dar prosseguimento ao processo de desfazimento.

8 PROGRAMAS DE COMPUTADOR (*SOFTWARES*)

8.1 Objetivo

Fixar diretrizes, responsabilidades e restrições quanto ao uso de *softwares* no âmbito do INT, de forma a proteger o Instituto de eventuais ações que venham a causar prejuízos financeiros ou denegrir sua imagem, bem como elaborar especificações técnicas para aquisição de *softwares* e assegurar ao usuário da rede do INT a manutenção e suporte aos mesmos.

8.2 Responsabilidade

8.2.1 Cabe à DINF a instalação e a elaboração das especificações técnicas de todos os *softwares* (Sistemas Operacionais, Aplicativos, Utilitários e Ferramentas) que serão adquiridos para utilização de uso geral na rede do INT;

8.2.2 No caso de aplicativos específicos de laboratório (instalação, especificação e manutenção) é de responsabilidade da chefia do laboratório.

8.3 Utilização

8.3.1 Sobre a propriedade e o direito de uso de *softwares* fica definido que:

8.3.1.1 Os *softwares* de propriedade do INT ou licenciados para o mesmo, não podem ser utilizados pelos usuários para a realização de atividades não relacionadas às suas atribuições funcionais;

8.3.1.2 A utilização de qualquer *software* no ambiente do INT está condicionada à análise prévia pelos técnicos da DINF, a fim de verificar a infra-estrutura necessária.

8.3.1.3 Os *softwares* adquiridos diretamente pelo usuário da rede do INT, em condições de legalidade, utilizados em serviços exclusivos e especiais poderão ser instalados desde que com conhecimento e autorização da DINF*;*

8.3.1.4 A utilização, por parte de qualquer usuário da rede do INT, de qualquer *software* não autorizado, não adquirido legalmente ou em desacordo com a Lei N.º 9.609 de 19 de dezembro de 1998, implicará a aplicação das medidas legais cabíveis por parte do INT.

8.3.2 Não é permitida a utilização de *softwares* de procedência desconhecida ou duplicados, sem a aquisição de licenças de uso do fabricante, fornecedor ou representante (programas piratas).

8.3.2.1 O uso de “programas piratas” acarreta os seguintes prejuízos ao INT:

8.3.2.1.1 Violar à Lei N.º 9.609 de 19 de fevereiro de 1998, que proíbe a reprodução, comercialização, importação e utilização de cópias de *softwares* feitos sem a devida autorização do titular dos direitos autorais;

8.3.2.1.2 Exposição negativa da imagem do INT perante a sociedade pelo descumprimento à lei;

8.3.2.1.3 Incidência de multas, pagamento de indenizações e outras penalidades previstas em lei;

8.3.2.1.4 Risco de incidência de vírus de computador, em função do desconhecimento de procedência.

8.3.2.1.5 Despadronização do parque de *softwares* da rede do INT;

8.3.2.1.6 Incompatibilidade com a plataforma de *softwares* adotada.

8.3.3 A avaliação de *softwares* pelos técnicos da DINF, antes da instalação nas estações de trabalho é obrigatória.

8.3.3.1 A prévia avaliação de *softwares* pelos técnicos da DINF evita que:

8.3.3.1.1 Sejam instalados *softwares* incompatíveis com o ambiente de trabalho do INT;

8.3.3.1.2 *Softwares* mal elaborados alteram arquivos nas estações de trabalho, deixando-as inoperantes ou prejudicando o funcionamento normal;

8.3.3.1.3 Sejam instalados componentes dispensáveis para a utilização do *software*, e que ocupam desnecessariamente, recursos da estação de trabalho (espaço no HD, memória, etc.).

8.3.3.2 A avaliação dos *softwares* pelos técnicos da DINF, antes da instalação nas estações de trabalho permite que:

8.3.3.2.1 Seja verificada a forma adequada de configuração do *software*;

8.3.3.2.2 Sejam identificadas as funções que estes *softwares* possuem, para que sejam dadas as devidas permissões para utilização na rede do INT.

8.3.3.2.3 O controle das licenças de produtos disponíveis para instalação nas estações de trabalho da rede do INT.

8.3.3.3 A utilização de *softwares* previamente avaliados apresenta as seguintes vantagens aos usuários da rede do INT:

8.3.3.3.1 Garantia de atualização em aquisição de novas versões;

8.3.3.3.2 Existência de documentação técnica;

8.3.3.3.3 Garantia de suporte técnico pela DINF e pelos fornecedores ou fabricantes dos *softwares*;

8.3.3.3.4 Produtos isentos de vírus de computador;

8.3.3.3.5 Legalidade.

8.3.4 Os *softwares* fornecidos por órgãos externos, sem ônus para o INT, deverão ser submetidos à DINF para teste, verificação de sua integridade e compatibilidade com os recursos existentes;

8.3.5 O desenvolvimento interno ou por terceiros, de novos *softwares* de uso geral a serem utilizados no INT, deverão seguir as orientações e a metodologia definida e utilizada pela DINF;

8.3.6 A utilização dos *softwares* desenvolvidos pela DINF, somente se dará com solicitação formal do interessado e autorização do gestor do referido sistema.

8.3.7 Os *softwares* desenvolvidos pela DINF somente poderão ser cedidos a outros órgãos mediante autorização do responsável pela DINF ou seu substituto.

9 DISPOSIÇÕES FINAIS

9.1 Caberá à DINF alterar este Manual a qualquer tempo, conforme necessidade, submetendo a nova versão à aprovação da Direção do INT, obrigando-se a disponibilizar as novas versões á todos os usuários de recursos computacionais do INT;

9.2 A chefia imediata ou superior, que tiver ciência do uso indevido dos recursos computacionais, comunicará o ocorrido ao Chefe de Divisão de Informática que determinará, dependendo da gravidade, abertura de processo administrativo cabível;

9.3 No caso de desrespeito às determinações citadas anteriormente, o agente público usuário de recursos computacionais estará sujeito a apuração da infração e conseqüente responsabilidade mediante a instauração do processo específico, assegurado o contraditório e a ampla defesa. Importa salientar que todos os usuários de equipamentos de informática estão sujeitos a:

9.3.1 Receber notificação, com cópia para sua respectiva chefia imediata, alertando acerca do mau uso dos recursos computacionais;

10 **ANEXOS**

10.1 Formulário de Criação de Usuários

INSTITUTO NACIONAL DE TECNOLOGIA
MINISTÉRIO DA CIÊNCIA E TECNOLOGIA

Solicitação de Criação de Usuário na rede do INT.

Data da Solicitação: ___/___/_____

Nome Completo do Solicitante: _____

Endereço: _____ Cidade: _____ Estado: ____

CPF: _____RG: _____

Unidade Alocada: _____

Função: _____

Sugestões de login (máximo três):
(os *logins* são elaborados com base no nome e sobrenome dos usuários. Ex.: Moysés Brito Dias → moyses.brito, moyses.dias)

_____@int.gov.br

_____@int.gov.br

_____@int.gov.br

Data de entrada em vigor: ___/___/____ Data de expiração do login: ___/___/____

Li e estou ciente dos termos de serviço de rede do INT.

_____ _____

Assinatura do Solicitante **Assinatura e Carimbo do Chefe**

_____

Assinatura do DARH

10.2 Termo Individual de Responsabilidade

INSTITUTO NACIONAL DE TECNOLOGIA
MINISTÉRIO DA CIÊNCIA E TECNOLOGIA

TERMO INDIVIDUAL DE RESPONSABILIDADE

Pelo presente instrumento, eu, _____, matrícula/identidade nº _____, perante o **Instituto Nacional de Tecnologia – INT**, na qualidade de usuário dos recursos de processamento da informação do INT, declaro estar ciente com a **Política de Utilização dos Recursos Computacionais** composta por suas Diretrizes Gerais, Normas, Procedimentos e Instruções, que estão disponíveis na INTRANET (http://intranet.int.gov.br).

Declaro, também, estar ciente de que os acessos por mim realizados à internet, bem como o conteúdo das mensagens enviadas através do Correio Eletrônico Institucional são monitorados automaticamente.

Declaro, ainda, estar ciente das minhas responsabilidades descritas nas normas da Política de Utilização dos Recursos Computacionais e que, a não observância desses preceitos, implicará na aplicação das sanções previstas nas Diretrizes Gerais desta Política.

Rio de Janeiro, _____de _____de_____.

_____

(Assinatura)

11 REFERENCIAS BIBLIOGRÁFICAS

- **LEI Nº 8.112 DE 14 DE NOVEMBRO DE 1990** – Regime Único dos Servidores Públicos;
- **LEI Nº 9.279, DE 14 DE MAIO DE 1996** – Regula direitos e obrigações relativos à propriedade industrial;
- **LEI Nº 9.610, DE 19 DE FEVEREIRO DE 1998** – Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências;
- **LEI FEDERAL Nº 8.159 DE 8 DE JANEIRO DE 1991** – Dispõe sobre a Política Nacional de Arquivos Públicos e Privados 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 Público Federal, e dá outras providências;
- **DECRETO Nº 26.209, DE 19 DE ABRIL DE 2000** – Cria a Delegacia de Repressão aos Crimes de Informática – DRCI e dá outras providências;
- **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;
- **LEI Nº 10.406, DE 10 DE JANEIRO DE 2002** – Institui o Código Civil;
- **DECRETO-LEI 2.848, DE 7 DE DEZEMBRO DE 1940** – Institui o Código Penal;
- **LEI Nº 9.983, DE 14 DE JULHO DE 2000** – Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências;
- **ABNT NBR ISO/IEC 17799:2005** – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação;
- **ABNT NBR ISO/IEC 27001:2006** – Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestão da Segurança da Informação – Requisitos;
- **MANUAL DE UTILIZAÇÃO DOS RECURSOS COMPUTACIONAIS DO MCT – Versão I / 2003** – Ministério da Ciência e Tecnologia. Referenciado na Norma Operacional SPOA nº 01 de 09 de janeiro de 2003;
- **BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO DO TCU** – Tribunal de Contas da União. Diretoria de Auditoria da Tecnologia da Informação. Brasília, 2003;
- **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO PRODERJ** – Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro. Portaria PRODERJ / PRE nº 172, de 14 de agosto de 2006.

12 GLOSSÁRIO

1. **Agentes públicos** - São todas as pessoas físicas incumbidas, definitiva ou transitoriamente, do exercício de alguma função estatal.
2. **Backup** - Cópia de segurança, geralmente mantida em determinado meio digital de armazenamento, que permite o resgate de informações importantes ou programas em caso de falhas.
3. **Bastidores dos elementos ativos de rede** - Local onde encontram-se os elementos ativos da **REDE DO INT** (*switches* , *hubs*).
4. **Download** – Transferência de arquivo. Baixar um arquivo da *Internet* para o computador.
5. **E-mail** – mensagem eletrônica. Uma caixa postal através da qual transmite-se mensagens, nas quais podem ser anexados arquivos de dados, imagens, etc. Fisicamente é um espaço em um servidor SMTP / POP para onde as mensagens são enviadas, e que são retiradas apenas pelo seu titular, através de uma senha.
6. **Fax/modem** - Equipamento acoplado ao computador para permitir envio de fax e conexão a *Internet*.
7. **Freeware** – *software* de domínio público, isento de taxas ou cobranças inclusive para atualização.
8. **FTP (File Transfer Protocol)** - Protocolo de Transferência de Arquivos.
9. **Hardware** - Parte física de um equipamento, como a CPU (gabinete), impressoras, vídeo, *scanner*, placas, cabos, etc.
10. **Internet** - Conjunto de rede de computadores interligados, de forma que os usuários a ela conectados possam usufruir de serviços de informação e comunicação de alcance mundial.
11. **Home Page** – Página de apresentação na *Internet*, a partir da qual se obtém acesso às demais informações que fazem parte daquele endereço (*site*).
12. **Intranet** - Aproveitamento, em escala interna, da tecnologia, ambiente gráfico, correio eletrônico, transferência de arquivos e de outras facilidades da *Internet*, permitindo a utilização das redes locais e remotas de modo semelhante.
13. **Lista de distribuição** - Grupo de usuários de Correio Eletrônico criado com objetivo de trocar informações sobre determinada área ou assunto relacionada as atividades desenvolvidas no trabalho.
14. **Login** – É o nome que o usuário utiliza para acessar o Servidor da Rede.
15. **Logon** – Processo de abertura da seção de trabalho do usuário, definido o perfil de acesso a determinados recursos computacionais.
16. **Logoff** – Processo de encerramento da seção de trabalho do usuário, fechando todos os acessos aos recursos computacionais.
17. **Impressoras Locais** – Impressoras conectadas nas estações de trabalho dos usuários e que atendem a um número restrito de pessoas.
18. **Impressoras Departamentais de Rede** – Impressoras conectadas ao Equipamento Servidor de Rede e que atendem aos usuários de uma determinada Unidade, exclusivamente para realização de impressões relativas ao trabalho.
19. **Notebook** - Tipo de computador portátil (leve e pequeno), geralmente, dotado de telas de cristal líquido e baterias recarregáveis.
20. **IMAP4 - (Internet Message Access Protocol)** - IMAP4 é a quarta versão do protocolo de acesso de mensagem de *Internet*. Ao contrário do POP, o IMAP permite que um usuário recupere de forma eficaz mensagens de mais de um computador.
21. **Modem ou Fax/Modem** – equipamento acoplado ao computador para permitir o envio de fax e conexão com a *Internet*.
22. **POP3 - (Post Office Protocol)** - Protocolo usado por programas de correio eletrônico para o recebimento de correspondência.
23. **Sala dos equipamentos Servidores de Rede** - Sala onde encontram-se todos os equipamentos servidores que estão em produção na **REDE DO INT**.

24. **Shareware** – *software* disponível para teste ou demonstração sem custo para o usuário. Geralmente é disponibilizado incompleto.
25. **Software** - se refere àquela porção do sistema digital que existe como dados binários e é executado ou usado pelo(s) microprocessador(es).
26. **Software Pirata** – *Software* com origem desconhecida ou produto de duplicação sem licença do fabricante.
27. **Spam** - envio de mensagem para um grande número de pessoas, sem que as mesmas a tenham solicitado.
28. **Site** – Endereço na *Internet*, cuja porta de entrada é a sua *Home Page*. O *site* do **INT** na *Internet* é http://www.int.gov.br/ e na *Intranet* http://*Intranet*.int.gov.br
29. **Usuário** - qualquer pessoa autorizada, que utiliza de qualquer forma ou para qualquer finalidade, algum recurso computacional do **INT**.
30. **Web** - Abreviatura para designar o *World-Wide-Web* (Rede Mundial de Computadores). Teia. O mesmo que WWW.