ESTADO DA PARAÍBA
SECRETARIA DE ESTADO DA RECEITA

PORTARIA Nº 083/GSER/2012
PUBLICADO NO DOU DE 03.04.12
REVOGADA PELA PORTARIA Nº 227/GSER
PUBLICADA NO DOE DE 14.10.14

Aprova a Política de Segurança da Informação de Tecnologia da Informação e o Manual do Usuário de Tecnologia da Informação da Secretaria de Estado da Receita – SER.

João Pessoa, 02 de abril de 2012.

O **SECRETÁRIO DE ESTADO DA RECEITA**, no uso das atribuições que lhe confere o art. 3º, inciso VIII, alínea “a”, da Lei nº 8.186, de 16 de março de 2007,

RESOLVE:

Art. 1º Aprovar a Política de Segurança da Informação de Tecnologia da Informação e o Manual do Usuário de Tecnologia da Informação da Secretaria de Estado da Receita – SER, como disposto nos Anexos I e II desta Portaria, respectivamente.

Art. 2º Revogam-se as disposições em contrário.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

MARIALVO LAUREANO DOS SANTOS FILHO
Secretário de Estado da Receita

ANEXO I DA PORTARIA Nº 083/GSER, DE 02/04/2012

A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DE TECNOLOGIA DA INFORMAÇÃO DA SECRETARIA DE ESTADO DA RECEITA - SER

CAPÍTULO I

DA SEGURANÇA ORGÂNICA DA GTI

Art. 1º A Política de Segurança da Informação de Tecnologia da Informação - TI obriga os servidores, prestadores de serviço, estagiários, quaisquer pessoas a serviço da Secretaria de Estado da Receita - SER e demais agentes públicos ou particulares que, por força de convênios, protocolos, acordos de cooperação e instrumentos congêneres, utilizem recursos de processamento da informação fornecidos pela instituição.

Art. 2º A Política de Segurança da Informação de TI tem por finalidade estabelecer as diretrizes de segurança do manuseio, tratamento e controle para a proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, pelos sistemas de informações administrados pela Gerência de Tecnologia da Informação, observadas as normas operacionais e de procedimentos no âmbito da SER.

CAPÍTULO II

DO OBJETIVO

Art. 3º A Política de Segurança da Informação de TI tem por objetivo prover a orientação para a segurança da informação, estabelecendo princípios e diretrizes para garantir a efetiva proteção dos dados, informações e conhecimentos gerados na SER.

CAPÍTULO III

DOS PRINCÍPIOS E DIRETRIZES

Art. 4º São princípios da Política de Segurança da Informação de TI:

I - a garantia ao direito pessoal e coletivo à intimidade e ao sigilo da correspondência e das comunicações individuais;

II - a proteção dos dados, informações e conhecimentos produzidos e armazenados na SER.

Art. 5º São diretrizes da Política de Segurança da Informação de TI:

I - a preservação da disponibilidade, integridade, confiabilidade e autenticidade dos dados, informações e conhecimentos que compõem os ativos de informação da SER;

II - a continuidade das atividades;

III - a economicidade da proteção dos ativos de informação;

IV - a pessoalidade e utilidade do acesso aos ativos de informação;

V - o seu conhecimento por parte de todos os usuários que utilizam os recursos de TI da SER, e a responsabilidade de cada um quanto ao cumprimento da mesma;

VI - a responsabilização do usuário pelos atos que comprometam a segurança do sistema da informação;

VII - a utilização das informações controladas pela GTI, apenas para os propósitos do serviço público.

CAPÍTULO IV

DA ABRANGÊNCIA

Art. 6º Por esta Portaria ficam abrangidos, e por ela obrigados, os servidores, prestadores de serviço, estagiários, quaisquer pessoas a serviço da SER e demais agentes públicos ou particulares que, por força de convênios, protocolos, acordos de cooperação e instrumentos congêneres, utilizem?se de recursos de processamento da informação fornecidos pela instituição.

Parágrafo único. A aplicação desta Política de Segurança da Informação de TI fica restrita aos procedimentos e ativos mantidos e controlados pela Gerência de Tecnologia da Informação.

CAPÍTULO V

DAS DEFINIÇÕES

Art. 7º Considera-se, para os fins desta Política de Segurança da Informação de TI:

I - **ameaça** – causa potencial de um incidente indesejado, podendo resultar em dano para um sistema ou organização;

II **- análise de risco e vulnerabilidades** – avaliação das ameaças, impactos e vulnerabilidades dos ativos de informação e da probabilidade de sua ocorrência;

III **- ativo de informação** – patrimônio composto por todos os dados, informações e conhecimentos obtidos, gerados e manipulados durante a execução dos sistemas e processos de trabalho da SER;

IV **- ativo de TI** – patrimônio composto por todos os equipamentos, programas e sistemas que compõem a infraestrutura de *hardware* e *software* da SER;

V **- controle de acesso** – procedimento destinado a impor restrições ao acesso aos dados e informações de um sistema;

VI **- controles de segurança** – ação ou conjunto de ações destinadas a mitigar ou minimizar ou transferir riscos dentro de uma organização;

VII **- disponibilidade** – princípio de segurança que trata da garantia de que pessoas autorizadas obtenham acesso à informação e aos recursos correspondentes, sempre que necessário;

VIII **- direito de acesso** – privilégio relacionado a um cargo, pessoa ou processo para ter acesso a um determinado ativo;

IX **- incidente de segurança** – qualquer evento ou ocorrência que promova uma ou mais ações tendentes a comprometer ou ameaçar a integridade, a autenticidade ou a disponibilidade de qualquer ativo gerenciado pela Gerência de Tecnologia de Informação;

X **- integridade** – princípio de segurança que trata da salvaguarda da exatidão e confiabilidade da informação e dos métodos de processamento;

XI **- meio de registro** – ativos de TI utilizados para manipulação dos ativos de informação;

XII **- proteção dos ativos** – processo pelo qual os ativos, e seus respectivos meios de registro, recebem classificação quanto ao grau de sensibilidade;

XIII **- responsabilidade** – rol de deveres da pessoa, decorrentes da função por ela exercida, em relação aos ativos da SER;

XIV **- risco** – probabilidade de que uma ameaça se concretize através da exploração de uma vulnerabilidade de um ou mais ativos;

XV **- sigilo** – princípio de segurança que estabelece que a posse e o acesso à informação sejam restritos às pessoas ou sistemas autorizados;

XVI **- usuários** – pessoas que detenham chave e senha de acesso aos ativos de informação da SER-PB, classificados como: servidores da SER, prestadores de serviço, estagiários, quaisquer pessoas a serviço da SER e demais agentes públicos ou particulares que, por força de convênios, protocolos, acordos de cooperação e instrumentos congêneres, executem atividade vinculada à atuação da Instituição;

XVII **- usuários externos** – pessoas que detenham chave e senha de acesso aos ativos de informação da SER, classificados como: contribuintes, sócios e representantes legais de empresas contribuintes, contadores ou servidores de outros órgãos da Administração Pública;

XVIII **- vulnerabilidade** – fragilidade de um ativo ou um grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO VI

REGRAS ESPECÍFICAS

Seção I

Da Organização

Art. 8º A Política de Segurança da Informação é o instrumento por meio do qual se regula a proteção dos dados, informações e conhecimentos da Instituição, com vistas à garantia de integridade, disponibilidade, conformidade e sigilo.

Art. 9º O gerenciamento dos ativos de informação deverá observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua.

Art. 10 O cumprimento desta política, bem como das normas operacionais e de procedimentos de Segurança da Informação na SER será auditado periodicamente, de acordo com os critérios definidos pelo Comitê Executivo de Tecnologia da Informação – CETI.

Art. 11 O acesso às informações, sistemas e instalações depende da apresentação de identificador único, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento.

Parágrafo único. O identificador pessoal e sua respectiva senha personalizam o usuário junto aos sistemas corporativos da SER, possuindo validade como registro das ações do mesmo.

Art. 12 A aquisição, a contratação de serviços de desenvolvimento, a instalação e o uso de sistemas e equipamentos devem ser homologados pela Gerência de Tecnologia da Informação.

Art. 13 O uso de recursos e informações pode ser controlado e monitorado pela SER para garantir o uso estrito e correto dos mesmos.

Art. 14 A política de segurança a que se reporta o presente Anexo deverá ser observada obrigatoriamente por todos aqueles que celebrarem compromissos com a SER.

Seção II

Gestão de Ativos

Art. 16 Os ativos de informação da SER devem ser inventariados e atribuídos aos respectivos responsáveis e seu uso deve estar em conformidade com os princípios e normas operacionais de segurança da informação.

Parágrafo único. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que contém.

Art. 17 Os ativos de informação da SER são destinados ao uso corporativo, sendo vedada a utilização para fins em desconformidade com os interesses institucionais.

Art. 18 É vedado ao usuário a utilização de quaisquer meios para acesso a sítios da *internet* inapropriados e não condizentes com o serviço público, bem como a disseminação de *e-mail* com igual conteúdo, por meio de equipamentos pertencentes ou não, no âmbito da SER, constituindo-se tal prática em infringência a Lei Complementar nº 58, de 30 de dezembro de 2003.

Seção III

Segurança de Pessoas

Art. 19 As responsabilidades pela segurança da informação devem ser definidas nas descrições de

cargos e funções, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimentos da SER.

Art. 20 Todos os usuários devem ser conscientizados e treinados nos procedimentos de segurança da informação em nível condizente com a realidade inerente às evoluções tecnológicas.

Art. 21 O controle operacional de uma atividade crítica não pode ser atribuição exclusiva de uma única pessoa.

Art. 22 Quando do afastamento, mudança de responsabilidades ou atribuições do usuário ou usuário externo, faz-se necessária a revisão imediata dos direitos de acesso e uso dos ativos.

Art. 23 Registros (log) de auditoria contendo atividades de usuários, exceções e outros eventos de segurança da informação serão produzidos e mantidos por período mínimo de cinco anos, para auxiliar no monitoramento de acessos, devendo ter tais registros proteção contra acessos e mudanças não autorizadas.

Art. 24 Deverá existir procedimento formalizado para o registro e cancelamento de usuários para garantir e revogar os acessos aos sistemas de informação e serviços.

Parágrafo único. O pedido para concessão de acesso, de usuário externo de outros órgãos da Administração Pública, se dará através de ofício emitido pelo chefe do respectivo órgão dirigido ao Secretário de Estado da Receita.

Art. 25 A definição de concessão e o uso de privilégios serão restritos e controlados pelo gestor do ativo.

Art. 26 Serão criados perfis de acesso, em função do cargo e/ou atividades exercidas, sendo definido o rol de concessões e privilégios de acordo com o perfil do usuário.

Parágrafo único. A concessão de acessos e privilégios fora do perfil do usuário poderá ser efetuada de forma excepcional, a pedido do superior hierárquico, com as devidas justificativas e o prazo da concessão ou por determinação do Secretário de Estado da Receita, nos casos de usuário externo de outros órgãos da Administração Pública.

Art. 27 A concessão e o gerenciamento das senhas serão controlados por processo formal e centralizado.

§ 1º É vedado aos usuários e usuários externos, o fornecimento de sua senha pessoal a outra pessoa.

§ 2º Os usuários e usuários externos deverão seguir as boas práticas para a criação e manutenção de suas senhas, de acordo com as instruções normativas vigentes.

Art. 28 Métodos mais criteriosos, para autenticação de usuários com acesso externo, deverão ser adotados tendo em vista a maior dificuldade em controlar este ambiente, inclusive, com a utilização de tecnologia de Certificação Digital.

Parágrafo único. Deverá haver inventário de todos os usuários externos autorizados, bem como a respectiva documentação e processo que lhe concedeu direito de acesso às informações e sistemas da SER.

Seção IV

Segurança de Áreas e Instalações

Art. 29 Todas as instalações da Gerência de Tecnologia da Informação devem ser classificadas de acordo com a importância e o nível de criticidade dos ativos ali mantidos.

Art. 30 Instalações que possuem ativos críticos ou sensíveis devem ser protegidas por perímetros de segurança definidos, com barreiras e controles de acesso apropriados.

Art. 31 Nenhum equipamento ou estação de trabalho pertencente à SER poderá ser removido ou transferido sem autorização expressa da Gerência de Tecnologia da Informação, devendo haver procedimento específico para cada caso.

Art. 32 Deve ser projetada e aplicada proteção física contra ameaças externas, do meio ambiente, de temperatura, umidade e problemas elétricos às instalações e aos equipamentos da Instituição.

Art. 33 Pontos de acesso à rede e outras formas de ingresso à informação deverão ser protegidos para evitar entradas de usuários não autorizados.

Art. 34 As redes que integram os serviços informatizados da SER deverão ser adequadamente gerenciadas, controladas e monitoradas para garantir a proteção contra ameaças, mantendo a segurança e a disponibilidade da mesma.

Seção V

Segurança de Informática

Art. 35 Os dados, as informações e os sistemas de informação da SER devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

Art. 36 É vedada, ao usuário ou usuário externo, a instalação de programas não autorizados pela Gerência de Tecnologia da Informação, bem como a desinstalação, alteração ou inserção de dados indevidos em programas homologados, nos equipamentos ou *softwares* pertencentes à SER, devendo haver controle por parte daquela Gerência sobre essa utilização.

Art. 37 Serão implantados sistemas centralizados de proteção contra códigos maliciosos, bem como procedimentos para a devida conscientização do usuário.

Art. 38 Os sistemas e recursos, que suportam funções críticas, devem assegurar a capacidade de recuperação nos prazos e condições definidas em situações de contingência.

Art. 39 O inventário sistematizado de toda a estrutura que serve de base para manipulação, armazenamento e transmissão dos ativos de processamento deve estar registrado e deve ser atualizado anualmente.

Art. 40 Requisitos para identificação e o uso de métodos criptográficos deverão ser empregados nas informações que trafeguem na rede, para assegurar a integridade das mesmas.

Art. 41 Acessos ao código fonte serão restritos e controlados.

Art. 42 Deve existir uma política de *backup* tanto para dados gravados na rede local, bem como para os *softwares* usados pela SER.

Art. 43 Procedimentos de manuseio de mídias removíveis deverão estar implementados em todos os setores da SER.

Art. 44 Os dados de entradas e saídas das aplicações deverão ser validados para garantir que são corretos e apropriados, e essas validações venha a ser incorporadas nas aplicações como padrão.

Seção VI

Gestão de Riscos, Incidentes e Continuidade do Negócio

Art. 45 A análise de risco deve ser realizada no âmbito da SER, visando identificar os ativos relevantes e determinar ações de gestão apropriadas.

Parágrafo único. A análise de risco deve ser atualizada anualmente, em função do inventário de ativos, mudanças, ameaças ou vulnerabilidades.

Art. 46 Deverá existir entre os setores da SER um canal apropriado para comunicação rápida e direta de eventos de segurança para que sejam tomadas as providências necessárias o mais breve possível.

Art. 47 Responsabilidades e procedimentos de gestão serão estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.

Art. 48 Violações de segurança devem ser registradas e analisadas periodicamente para os propósitos de caráter corretivo, legal e de auditoria.

Parágrafo único. Os registros referidos no *caput* devem ser protegidos e armazenados de acordo

com a sua classificação.

Art. 49 Deverá ser instituído o Plano de Contingência para manutenção e recuperação das operações, bem como para assegurar a disponibilidade da informação em nível de acesso aceitável e numa escala de tempo razoável em cada serviço após a incidência da interrupção ou falha do processo crítico de negócio.

Parágrafo único. O Plano de Contingência deverá ser testado e atualizado, anualmente, de forma a assegurar sua permanente atualização e efetividade.

Art. 50 Quando houver uma ação de acompanhamento envolvendo usuário, usuário externo ou organização, após um incidente de segurança da informação, evidências serão coletadas, armazenadas e apresentadas para investigações posteriores.

Art. 51 Modificações em pacotes de *softwares* devem ser limitadas às mudanças extremamente necessárias e essas mudanças serão controladas em ambiente de testes inicialmente.

CAPÍTULO VII

RESPONSABILIDADES

Art. 52 A presente Política de Segurança da Informação, as normas operacionais e os procedimentos de segurança obrigam todos os que executem atividades através do uso de informações e sistemas da SER.

Seção I

Das Competências

Art. 53 Compete ao Comitê Executivo de Tecnologia da Informação – CETI:

I – assegurar que a implementação dos controles de segurança da informação tenha uma coordenação e permeie toda a organização;

II - pleitear os recursos necessários para a implementação e gestão da Política de Segurança da Informação da SER.

Art. 54 Compete à Gerência de Tecnologia da Informação:

I – sempre que necessário, propor modificações à Política de Segurança da Informação;

II – definir estratégias para a implantação da Política de Segurança da Informação;

III – emitir orientações operacionais e de procedimentos de segurança da informação aos usuários;

IV – planejar e coordenar a execução dos programas, planos, projetos e ações de segurança;

V - apurar os incidentes de segurança críticos e encaminhar os fatos apurados para aplicação das penalidades previstas;

VI – supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação;

VII – manter a análise de risco atualizada, refletindo o estado corrente da organização;

VIII – identificar controles físicos, administrativos e tecnológicos para mitigação do risco;

IX – recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança, determinando aos respectivos gestores as ações corretivas ou de contingência em cada caso;

X – promover a conscientização e propor o treinamento dos usuários em segurança da informação;

XI - produzir relatórios sintéticos de incidentes de segurança da informação para o CETI;

XII - auditar a utilização pelos usuários dos acessos realizados a sistemas, aplicativos e rede externa.

Parágrafo único. Fica facultado ao Gerente de Tecnologia da Informação, delegar quaisquer de suas competências, definidas nesta Portaria, aos responsáveis pelos demais setores da Gerência.

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Seção I

Penalidades

Art. 55 O não cumprimento das determinações da Política de Segurança da Informação sujeitam o infrator às penalidades previstas na legislação.

Subseção I

Processo Administrativo Disciplinar

Art. 56 No caso de infração cometida por servidor do Governo do Estado da Paraíba será instalado o respectivo Processo Administrativo Disciplinar.

Art. 57 As provas contra o usuário poderão ser coletadas de seu ambiente de trabalho, tanto físicas quanto computacionais.

Art. 58 Toda ferramenta, acessos, e equipamentos dados ao usuário para que este exerça sua função é de propriedade da SER, sob controle da Gerência de Tecnologia da Informação, sendo

estes meios passíveis de auditorias internas e externas.

Seção II

Revisão da Política de Segurança

Art. 59 A Política de Segurança de que trata esta Portaria deve ser revisada e atualizada periodicamente no máximo a cada ano, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata, sendo a primeira revisão realizada em seis meses após sua publicação, devendo o mesmo procedimento ser aplicado às instruções normativas que estejam amparadas por esta política.

Art. 60 A Política de Segurança da Informação e o Manual do Usuário de Tecnologia da Informação serão disponibilizados a todos os servidores e prestadores de serviços da SER, estabelecendo Normas Operacionais e de Procedimentos, cuja manutenção e atualização ficarão a cargo da Gerência de Tecnologia da Informação, sob aprovação do Comitê Executivo de Tecnologia da Informação - CETI.

Art. 61 O CETI atuará como Comitê de Segurança da Informação, podendo exercer as atribuições do Comitê Gestor de Mudanças e será responsável pela supervisão da implementação da Política de Segurança da Informação.

Art. 62 Os procedimentos para a execução desta política poderão ser detalhados e efetuados através de instruções normativas ou manuais de procedimentos.

Art. 63 Para as atribuições previstas nesta Portaria e demais instruções dela advindas ao Secretário de Estado da Receita, fica sub-rogado o Secretário Executivo da Secretaria de Estado da Receita.

MARIALVO LAUREANO DOS SANTOS FILHO
Secretário de Estado da Receita

ANEXO II DA PORTARIA Nº 083/GSER, DE 02/04/2012

MANUAL DO USUÁRIO DE TECNOLOGIA DA INFORMAÇÃO

Sr(a). usuário(a),

Este manual é parte integrante da Política de Segurança da informação da Secretaria de Estado da Receita.

Como forma de auxiliar no entendimento dos parâmetros e modos de uso seguro das informações que são armazenadas e transitam em meio eletrônico, foi criada a Política de Segurança da Informação, cujo detalhamento para o usuário se dá através deste Manual.

Este documento não representa um trabalho pronto e acabado, mas de orientação ao disponibilizar informações sobre a utilização quanto ao bom uso da *Internet* e do *e-mail*.

Contamos desde já com a contribuição de todos os servidores e prestadores da SER para o aprimoramento do trabalho. As sugestões e críticas podem ser dirigidas ao seguinte *e-mail*: gti.sugestoes@receita.pb.gov.br.

1. EQUIPAMENTOS (*HARDWARE*) E PROGRAMAS/APLICATIVOS (*SOFTWARE*)

Os microcomputadores, periféricos e os programas utilizados são patrimônio do Estado, com uso voltado exclusivamente ao serviço público.

O mau uso, depredação ou inutilização, antes de ser uma conduta passível de punição por indisciplina funcional, fere a ética profissional. Preservar o patrimônio público é uma atitude de respeito ao contribuinte.

2. RECOMENDAÇÕES DURANTE O EXPEDIENTE

Todas às vezes que se ausentar do computador faça o bloqueio da seção, através das teclas “CTRL + ALT + DEL” (bloquear computador). Isto é importante para que outro usuário, até de forma inadvertida, não utilize a sua chave de acesso.

Caso queira sair da seção para que outro usuário possa utilizar o computador, basta usar a mesma sequência de teclas, escolhendo a opção “fazer *logoff*”.

3. A *INTERNET* E O *E-MAIL*

A *internet* trouxe mais agilidade, interatividade e ‘abriu as portas’ para o mundo, mas precisa de atenção e certos cuidados no uso.

A análise das diversas formas de utilização da *internet* mostra que muitos usuários ainda acessam páginas da rede de forma indiscriminada, com objetivos alheios aos preceitos de crescimento individual e intelectual. Acessos aos sítios de conteúdo discordante dos preconizados no serviço público ou simplesmente tratar a ferramenta como mecanismo de entretenimento pessoal não condizem com os trabalhos desenvolvidos na Secretaria de Estado da Receita.

Essas condutas refletiram diretamente na mudança de postura adotada na segurança interna dos computadores da SER. O acesso a esses sites ou o uso de programas específicos pode tornar a estrutura vulnerável e passível de invasão por *hackers* (piratas da *internet*), de ‘vírus’ de computador e de uma infinidade de outros perigos virtuais.

4. DIRETRIZES QUANTO AO USO DA *INTERNET*

A *internet* deve ser utilizada para fins de complemento às atividades do setor, pois traz mais agilidade e rapidez na busca de informação e comunicação, além de crescimento intelectual dos servidores. No caso dos pesquisadores, a ferramenta proporciona busca por informações diversificadas que contribuem para o desenvolvimento dos trabalhos.

Jamais deve ser utilizada para a realização de trabalhos de terceiros ou de atividades paralelas, bem como para acesso a sítios de conteúdo pornográfico ou de estímulo a preconceitos de etnia, cor, sexo, orientação sexual e opção religiosa.

O uso para fins pessoais, como a consulta a movimento bancário ou acesso a *e-mail* pessoal pode ser realizado, desde que não prejudique o bom andamento dos trabalhos e com o consentimento do chefe ou responsável pelo setor.

São passíveis de auditoria, pelo administrador de segurança da Gerência de Tecnologia da Informação, os acessos realizados pelos usuários como forma de controle e monitoração do uso da rede, devendo alertá-los sobre eventuais excessos de consumo da banda de comunicação ou utilização inapropriada da ferramenta.

5. A REALIZAÇÃO DE *DOWNLOADS*

O processo de realização de *downloads* consome boa parte da banda de navegação da rede e, quando realizado em demasia, congestiona o tráfego e torna a navegação para os demais usuários

inviável.

Downloads grandes, por exemplo, podem congestionar o tráfego e comprometer sistemas que funcionam *on-line*. Muitas vezes os sistemas ficam 'lentos' e não sabemos porquê. Assim, não é permitido nas estações em uso na SER a realização de *download* e utilização de aplicativos que não sejam homologados pela GTI, tais como *freeware* ou *shareware* disponível na *internet*.

6. EXECUÇÃO DE JOGOS, RÁDIOS E TV *ON-LINE*

Uma vez que não existe qualquer pertinência com as finalidades institucionais da Administração Pública, é proibida a execução, *on-line* ou não, de jogos, músicas, rádios, TV's, programas de compartilhamento de arquivos (P2P) ou congêneres. Essa prática também consome grande parcela da banda da rede, dificultando a execução de outros serviços da SER que necessitam deste recurso, salvo exceções, devidamente regulamentadas.

7. SENHAS DE ACESSO

Somente poderão ter acesso à *internet* usuários que tenham sido credenciados com *login* e senha.

A senha de acesso tem caráter pessoal e intransferível, cabendo ao seu titular total responsabilidade quanto ao seu sigilo.

A prática de compartilhamento de senhas de acesso é terminantemente proibida e o titular que fornecer sua senha a qualquer outra pessoa responderá pelas infrações que venham a ser cometidas.

Caso o usuário desconfie que sua senha não é mais segura, ou de seu domínio exclusivo, deverá alterá-la ou solicitar à Gerência de Tecnologia da Informação a inclusão de nova senha.

É recomendável na escolha da senha que não seja utilizada a seqüência de fácil dedução como datas de aniversário, número da matrícula etc. Utilize senhas com no mínimo 08 (oito) caracteres, sendo pelo menos uma letra, um número e um caractere especial. Exemplo: *A123@123.*

8. RECOMENDAÇÕES

Quando for acessar algum sítio na *internet*, de preferência digite o endereço completo, evitando clicar em *links* que possam levar a páginas fraudulentas.

Nunca utilize *softwares* ou procedimentos para tentar burlar o sistema de bloqueios de páginas na *internet*. Essas práticas são passíveis de punição conforme definido na Política de Segurança.

9. RECOMENDAÇÕES SOBRE O USO DO *E-MAIL*

Não abrir anexos de *e-mail* com as extensões **.bat**, **.exe**, **.src**, **.lnk** e **.com**, ou de quaisquer outros formatos alertados pela Gerência de Tecnologia da Informação.

Desconfiar de todos os *e-mails* com assuntos estranhos e/ou em língua estrangeira.

Não reenviar *e-mails* do tipo corrente, aviso de vírus, avisos da Web, criança desaparecida ou doente, *sites* de compras, conteúdo pornográfico, *spam* etc.

Não utilizar o *e-mail* corporativo para assuntos pessoais ou cadastrá-lo em listas de discussões fora da SER.

Não clique em *links* recebidos por *e-mail*, nem em *links* para cancelar o recebimento de *e-mails* enviados por fontes desconhecidas.

Não execute arquivos recebidos por *e-mail* ou via serviços de mensagens instantâneas ou *chats*.

Evitar o envio de anexos ‘pesados’.

Adotar o hábito de ler sua caixa de *e-mails* diariamente (pela manhã e à tarde), como forma de evitar acúmulos de *e-mails*.

Utilizar o *e-mail* para comunicações oficiais internas, principalmente naquelas que não necessitem, obrigatoriamente, do meio físico escrito. Isto diminui o custo com impressão e aumenta a agilidade na entrega e leitura do documento.

Havendo necessidade de envio de *e-mails* em grande quantidade (difusão), deverá encaminhar pedido à Gerência de Tecnologia da Informação solicitando autorização.

É de exclusiva responsabilidade do usuário o conteúdo de seus arquivos, bem como o mau uso por terceiros de seu *e-mail*. Por ser o *e-mail* corporativo e não pessoal, o mesmo é passível de monitoramento de forma impessoal, para assegurar o cumprimento das regras aqui descritas.

10. USO DE *SOFTWARES* DE COMUNICAÇÃO INSTANTÂNEA

O uso de *softwares* de comunicação instantânea, ou de qualquer outro mecanismo que venha promover serviço semelhante, será regulamentado por norma operacional da Gerência de Tecnologia da Informação. Mensageiros instantâneos do tipo MSN, Yahoo Messenger, Google Talk e semelhantes somente poderão ser liberados mediante prévia autorização da GTI.

11. USO DE MÍDIA REMOVÍVEL

Evite trazer Cd’s, DVD’s ou *pen-drivers* de fora da instituição. Você pode estar trazendo ‘vírus’ de outros equipamentos para a sua estação de trabalho e, conseqüentemente, poderá infectar não só o seu equipamento, como também a rede interna da SER.

MARIALVO LAUREANO DOS SANTOS FILHO
Secretário de Estado da Receita