SUMÁRIO

SEPARATA DO BOLETIM DE SERVIÇO Nº 18

ANO XX

Setembro - 2007

APRESENTAÇÃO

Esta Separata do Boletim de Serviço destina-se a publicação de atos oficiais da FUNAI não publicados em Boletins de Serviço no mês de setembro de 2007.

Os atos nele publicados têm validade jurídica na forma do disposto no Decreto nº 96.496, de 12 de agosto de 1988, ressalvados aqueles de publicação obrigatória no Diário Oficial da União, e deverão ser registrados e cumpridos independentemente de qualquer comunicação ou expediente complementar.

Brasília, 18 de outubro de 2007.

PORTARIA Nº 928/PRES, de 21 de setembro de 2007.

O PRESIDENTE DA FUNDAÇÃO NACIONAL DO ÍNDIO - FUNAI, no uso das atribuições que lhe são conferidas pelo Estatuto, aprovado pelo Decreto nº 4.645, de 25 de março de 2003 e pela Portaria MJ nº 542, de 21 de dezembro de 1993, e,

Considerando a necessidade de formalizar as práticas de Segurança da Informação, visando garantir a integridade, disponibilidade e autenticidade dos dados e informações disponibilizadas no âmbito desta Fundação,

R E S O L V E :

Art. 1º Aprovar, na forma do Anexo, a Política de Segurança da Informação da Funai.

Parágrafo único. A Política de que trata este artigo, visa prover a FUNAI de norma para Segurança da Informação, estabelecendo responsabilidades e diretrizes, bem como atitudes adequadas para manuseio, tratamento, controle e proteção contra a indisponibilidade, a divulgação, a modificação e o acesso não autorizados de informações e dados.

Art. 2º As diretrizes de segurança da informação estabelecidas nesta Portaria são aplicáveis tanto às informações armazenadas quanto em trânsito e devem ser seguidas por todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço incumbindo a cada um a responsabilidade e o comprometimento para a sua aplicação.

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

MÁRCIO AUGUSTO FREITAS DE MEIRA
Presidente

ANEXO (Portaria nº 928/Pres, de 21.09.2007)

NORMAS DE UTILIZAÇÃO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO DISPONIBILIZADOS NA FUNAI SEDE E EM SUAS UNIDADES

SUMÁRIO

FINALIDADE

Este documento visa definir norma de segurança da informação, em conformidade com a legislação brasileira aplicável, estabelecendo responsabilidades e atitudes adequadas para manuseio, tratamento, controle e proteção contra indisponibilidade, divulgação, acesso e modificação não autorizados de informações e dados e de equipamentos, providos pela FUNAI, por intermédio da sua Coordenação Geral de Documentação e Tecnologia da Informação e por suas unidades desconcentradas.

ABRANGÊNCIA

Esta norma aplica-se a toda a FUNAI, em sua Sede, Administrações Regionais e a todos os usuários, inclusive externos, servidores públicos ou equiparados, prestadores de serviços e estagiários.

FREQÜÊNCIA DE REVISÃO

Esta norma deve ser revisada a cada ano, pelo menos.

LEGISLAÇÃO

- Lei nº 9.983, de 14 de julho de 2000, que altera o Código Penal Brasileiro, já prevê penas para os casos de violação de integridade e quebra de sigilo de sistemas informatizados ou banco de dados da Administração Pública.
- Decreto nº 3.505, de 13.06.2000, instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- Lei nº 8.112, de 11 de dezembro de 1990, dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.
- Decreto-Lei nº 2.848, de 7 de dezembro de 1940, código penal brasileiro.
- Lei nº 8.159, de 08 de janeiro de 1991, dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências e alterações legais.
- 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.

CONCEITOS

5.1 AMEAÇA – uma possível violação da segurança de um sistema.

5.2 ANTIVÍRUS – programa que tem a função de detectar e remover arquivos ou aplicativos nocivos ao sistema.

5.3 ÁREAS DE SEGURANÇA - são locais de processamento ou armazenamento de informações projetadas para prevenir acesso não autorizado, dano e interferência às informações e instalações físicas, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso.

5.4 CAIXA POSTAL - área pré-definida que armazena as mensagens de Correio Eletrônico. Cada usuário possui uma área específica, não compartilhada com outros usuários. Sobre a referida área pode incidir limites e configurações de armazenamentos definidas pela área de CGDTI.

5.5 CTI – Coordenação de Tecnologia da Informação, antiga **CGI.**

5.6 ENDEREÇO DE CORREIO ELETRÔNICO - é a representação simbólica que torna possível a identificação unívoca do usuário, classificado em:

5.6.1 Endereço de Correio Eletrônico Individual é aquele utilizado por pessoa física seja servidor ou equiparado, empregado, prestador de serviços ou estagiário;

5.6.2 Endereço de Correio Eletrônico Institucional é aquele utilizado por uma unidade administrativa e suas subdivisões ou grupo de trabalho, formalmente instituído na FUNAI.

5.7 **ESTAÇÃO DE TRABALHO** – Computador projetado para ser usado em uma mesa de trabalho ligado a redes corporativas, podendo ser estação fixa (mesa de trabalho) ou estação móvel (notebook).

5.8 **IDENTIFICAÇÃO DO USUÁRIO** - é a forma como o usuário é cadastrado pela administração do Correio Eletrônico, em que o conjunto, Identificação do Usuário e Senha, permite que ações e ferramentas sejam utilizadas de acordo com o perfil do usuário conforme as regras estabelecidas no item 28.

5.9 **INTERNET –** Rede mundial de computadores na qual o usuário pode, a partir de um computador, caso tenha acesso e autorização, obter informações de qualquer outro computador que também esteja conectado à rede. O protocolo padrão utilizado é o TCP/IP. Tradicionalmente possui algumas aplicações principais: e-mail (correio eletrônico), ftp (transferência de arquivos) e www (World Wide Web).

5.10 **INTRANET –** Rede fechada, que funciona interligando os computadores de uma mesma empresa, no mesmo prédio, ou de uma corporação, nos escritórios de diversos países, ou de uma associação de pessoas unidas por algum objetivo específico. A diferença é que a intranet não pode, diferentemente da Internet, ser acessada por alguém que não seja parte de um grupo específico.

5.11 **LISTA DE DISCUSSÃO** - é um grupo de usuários de Correio Eletrônico formado com o objetivo de trocar informações relacionadas a uma determinada área ou assunto. Pode ser estritamente interna ao órgão, ou de conhecimento público.

5.12 **LOG** – Processo de registro de informações sobre as atividades ou eventos (tais como login, tráfego) em um determinado sistema computacional. As logs são utilizadas para permitir recuperação nas situações de falhas, auditoria nas situações de violações de segurança e contabilização de uso de recursos.

5.13 **MENSAGEM DE CORREIO ELETRÔNICO** – registro eletrônico ou mensagem criada, enviada, encaminhada, respondida, transmitida, arquivada, mantida, copiada, exibida ou impressa por serviço de Correio Eletrônico.

5.14 **MODEM** – equipamento capaz de realizar modulação e demodulação de sinais para transmissão de dados. Normalmente é utilizado para conexões a redes de longa distância empregando linhas telefônicas.

5.15 **RECURSOS DE TI** - hardware, software, dado e informação, serviço provido por meio eletrônico e meio de comunicação.

5.16 **REDES DE COMPUTADORES** - é a união de dispositivos eletrônicos capazes de trocar dados e compartilhar recursos, interligados por um sistema de comunicação.

5.17 **SERVIÇO DE CORREIO ELETRÔNICO** - é um sistema de mensageria utilizado para elaborar, enviar, encaminhar, responder, transmitir, arquivar, manter, copiar, recuperar, exibir ou imprimir informações com o propósito de comunicação entre meios eletrônicos ou sistemas informatizados ou entre pessoas ou grupos.

5.18 **SERVIDOR –** Computador que fornece um ou mais serviços a outro computador, em uma rede, administrando arquivos e operações dessa rede.

5.19 **SISTEMA DE TELEMÁTICA** – é o conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens; que possibilitam a agregação dos recursos de Tecnologia da Informação e Telecomunicações em forma integrada.

5.20 **SMTP** – (Simple Mail Transfer Protocol) é utilizado para transferir mensagens de correio eletrônico entre sistemas da Internet e Intranet.

5.21 **SPAM** – Envio de mensagem comercial ou do tipo corrente não solicitada pelos usuários. Pode ocorrer de duas formas:

a) Quando diversas mensagens são enviadas para um único local, como caixa de correio de usuário;

b) Quando grupos de usuários constantes em fóruns ou listas de debates são bombardeados com mensagens comerciais ou correntes.

5.22 **USUÁRIO** – servidores efetivos, os ocupantes de cargos em comissão, os funcionários ou empregados requisitados ou cedidos de outros órgãos públicos, além daqueles que, por força de lei, contrato ou qualquer outro ato jurídico, prestem serviços de natureza permanente, temporária ou excepcional, ainda que sem retribuição financeira, desde que vinculados direta ou indiretamente a FUNAI, bem como a unidade administrativa e suas subdivisões ou grupo de trabalho reconhecido e habilitado pela administração para utilizar os serviços disponibilizados pela CGDTI. Sinônimo: conta de usuário.

5.23 VÍRUS – Programa de computador destrutivo que tem a habilidade de auto-replicar e infectar partes do sistema operacional ou de outros programas, com o intuito de causar a perda ou dano nos dados.

Os meios mais conhecidos de propagação são:

a) Arquivos anexados em e-mails, podendo ser programas executáveis (extensão - .exe), jogos, arquivos de textos ou imagens;

b) Instalação de programas piratas e;

c) Disquetes ou CD's de origem duvidosa.

RESPONSABILIDADE

A atual CGDTI – Coordenação de Documentação e Tecnologia da Informação, nos termos do Regimento Interno, é a responsável pela gestão dos sistemas de informação e dos recursos de TI e de transmissão de dados da FUNAI, exceto quanto aos sistemas oficiais do Governo Federal, que, por força de norma própria, determinem o contrário.

A CGDTI é também responsável pela coordenação e autorização da utilização de qualquer recurso computacional dentro da FUNAI.

A aquisição e/ou contratação de serviços relativos a recursos computacionais pressupõe conhecimento prévio por parte da CGDTI e posterior autorização de instância superior.

CREDENCIAMENTO

Para utilizar qualquer recurso de TI da FUNAI é necessário o credenciamento através de criação de conta com senha pessoal, mediante solicitação formal, da chefia imediata, através do encaminhamento do documento Termo de Responsabilidade e Manutenção de Sigilo, devidamente preenchido e assinado, conforme modelo previsto (item 28) nesta Norma.

SEGURANÇA DOS EQUIPAMENTOS

Todos os computadores conectados devem obedecer aos procedimentos padronizados de segurança estabelecidos pela CGDTI.

Deve ser implementado controle de acesso físico aos locais onde se encontram instalados os equipamentos sensíveis de TI (Servidores de rede, Switchs, Roteadores e etc.).

É proibida a utilização de recursos pessoais de TI no ambiente de trabalho.

Os equipamentos e mídias levados para fora das instalações da FUNAI, não devem ser deixados desprotegidos e sem custódia em áreas públicas.

Nas viagens, os computadores portáteis devem ser carregados como bagagem de mão de modo discreto, sempre que possível.

AMBIENTE DE TRABALHO

Papéis e mídias de computador devem ser guardados em gavetas adequadas, com fechaduras, e/ou outras formas seguras de armazenamento, especialmente fora do horário normal de trabalho.

Sempre que se ausentar de seu posto de trabalho o usuário deve bloquear o acesso de terceiros às informações sob sua responsabilidade, utilizando-se das teclas Ctrl + Alt + Del e posteriormente clicando na tecla bloquear computador.

As estações de trabalho devem ser desligadas quando fora de uso.

Informações sensíveis e classificadas, quando impressas, devem ser imediatamente retiradas da impressora.

Deve ser evitado o trabalho sem supervisão em áreas de segurança.

Não é permitido o uso de equipamentos de captura de imagens e áudio em áreas de segurança, salvo se formalmente autorizado.

As áreas de segurança desocupadas devem ser mantidas fisicamente fechadas e verificadas periodicamente.
É proibido o consumo de bebidas e alimentos em áreas de segurança.

IDENTIFICAÇÃO E AUTENTICAÇÃO DE USUÁRIO

Todos os usuários (incluindo o pessoal de suporte técnico, como operadores, administradores de rede, programadores de sistema e administradores de banco de dados) devem utilizar um identificador único (conta de usuário) para uso pessoal e intransferível, de modo que as atividades possam ser rastreadas.

O acesso especial a informações, sistemas, serviços e outros privilégios decorrentes só podem ser usados para o fim a que se destinam. Informações obtidas por meio de direitos especiais e privilégios devem ser tratadas com o grau de classificação de acordo com o Nível de Proteção preconizado pela PSI - Política de Segurança da Informação.

O tempo máximo de inatividade de uma conta é de 3 (três) meses. Após 1 (um) mês o usuário será avisado da data de desabilitação da mesma.

O horário de uso dos recursos computacionais poderá ser limitado de acordo com a real necessidade de acesso e perfil do usuário.

USO DE SENHAS

As senhas fornecem um meio de validação da identidade do usuário e conseqüentemente o estabelecimento dos direitos de acesso para os recursos ou serviços de TI. Todos os usuários devem:

- manter o sigilo de sua senha pessoal e das senhas de grupos de trabalho;
- não registrar suas senhas em papel ou outro suporte, a menos que possa ser guardado de forma segura (exemplo: dentro de um cofre);
- alterar a senha sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;
- selecionar senhas de qualidade, com tamanho mínimo de 6 caracteres e no máximo 11 caracteres, que sejam:

a) fáceis de lembrar;

b) que sejam originadas de elementos que outras pessoas não possam facilmente adivinhar ou obter a partir de informações pessoais. Deve-se evitar por exemplo:

a. nome do usuário;
b. identificador do usuário (ID), mesmo que seus caracteres estejam desordenados;
c. nome de membros de família ou de amigos;
d. nomes ou lugares em geral;
e. nome do sistema operacional ou da máquina que está sendo utilizada;
f. datas;
g. números de telefone, cartão de crédito, de carteira de identidade ou de outros documentos pessoais;
h. placas ou marcas de carro;
i. palavras que constam de dicionários em qualquer idioma;
j. letras ou números repetidos;
k. letras seguidas do teclado do computador, por exemplo, ASDFG ou YUIOP;
l. objetos ou locais que podem ser vistos a partir da mesa do usuário, por exemplo o nome de um livro na estante ou o nome de uma loja vista pela janela;
m. que tenham caracteres idênticos consecutivos ou de grupos de caracteres somente numéricos ou alfabéticos.

É conveniente escolher senhas que possam ser digitadas rapidamente, dificultando que outras pessoas, a certa distância ou por cima de seus ombros, possam identificar a seqüência de caracteres.

As senhas deverão ser alteradas a cada 3 (três) meses sendo vedada a reutilização de senhas antigas;

É proibida a inclusão de senhas em processos automáticos de acesso ao sistema, por exemplo, armazenadas em macros ou teclas de função. Exemplo: lembrador de senhas do Windows Internet Explorer.

Usuários que precisarem ter acesso a múltiplas plataformas ou serviços ao utilizar uma única senha, esta deve ter o grau de complexidade e de proteção compatíveis com o de maior nível de sigilo.

A senha de acesso aos recursos de TI é pessoal e intransferível, sendo de responsabilidade e uso exclusivo do titular.

Os usuários são responsáveis por qualquer atividade desenvolvida por meio das suas contas e pelos eventuais custos e conseqüências decorrentes de sua má utilização.

CONTROLE DE ACESSO

Cabe ao responsável de cada unidade providenciar o acesso físico e lógico aos usuários sob sua responsabilidade, conforme necessidade dos mesmos.

Os usuários terão os seguintes níveis de acesso:

Nível 01: Simples usuário do domínio, com acesso pré-configurado a Intranet, sendo as demais opções bloqueadas na diretiva de segurança. Mediante autorização, por escrito, do gestor da informação ou do chefe imediato, tem acesso ás pastas no servidor de arquivos, sistemas específicos, correio eletrônico e à Internet;

Nível 02: Usuário com todos os acessos/privilégios do nível 01 e mais a capacidade de instalar impressoras, scanners, configurar e-mail no MS Outlook 2000/2003. Demais alterações são restritas.

Nível 03: Usuário com os privilégios do nível 02 e mais a permissão para instalar programas, alterar configurações em programas pré-instalados em estações, adicionar ou remover estações no domínio FUNAI_SEDE e criar e desbloquear usuários nível 01 e 02;

Nível 04: Usuário com os privilégios do nível 03 e mais as seguintes autorizações: instalar, configurar e alterar serviços em servidores, administrar banco de dados, criar relação de confiança entre domínios, conectar-se remotamente às regionais, configurar roteadores e criar usuários de níveis abaixo;

Nível 05: Usuário com os privilégios do nível 04 e mais as seguintes autorizações: fazer alterações e intervenções em todos os serviços corporativos e em todos os domínios quando necessário;

Nível 06: Usuário específico para o acesso ao conteúdo de e-mail e/ou arquivos de todas as categorias de usuários;

Nível E1 (externo 1): sistema específico;

Nível E2 (externo 2): conta de e-mail;

12.3 As senhas dos usuários níveis 04,05 e 06, como também para toda alteração dessas senhas, as mesmas serão encaminhadas a CGDTI, em envelope lacrado, o qual só será violado, mediante Termo Circunstanciado, quando por motivo de força maior, ou fato superveniente, estiver o detentor original da senha impossibilitado de acessar o sistema.

12.4 O responsável pela unidade deve providenciar o bloqueio dos acessos físicos e lógicos aos usuários sob sua responsabilidade quando necessário.

12.5 O responsável pela unidade deve garantir o acompanhamento de um visitante ou recurso externo que manipule direta ou indiretamente a informação sob sua responsabilidade.

12.6 O compartilhamento de informações deve ser efetuado de acordo com a sua classificação e importância.

12.7 O número de tentativas de entrada nos sistemas será limitado a 3 (três) tentativas. Após a terceira tentativa a conta será bloqueada.

12.8 As contas com senhas em desconformidade com o Capítulo 11 desta norma serão desabilitadas.

CÓPIAS DE SEGURANÇA

A realização de cópias de segurança dos dados contidos nas estações de trabalho é de responsabilidade do usuário.

A realização de cópias de segurança dos dados contidos nos computadores-servidores da rede é de responsabilidade da CTI – Coordenação de Tecnologia da Informação.

PREVENÇÃO CONTRA USO INDEVIDO DE RECURSOS DE TELEMÁTICA

Os recursos do Sistema de Telemática da FUNAI, incluindo, equipamentos, utilitários, aplicativos, sistemas operacionais, mídias de armazenamento, contas em servidores, endereços de Correio Eletrônico, navegação na Internet e Intranet, serviço de transferências de dados, terminal virtual, comunicação interativa e outros, devem ser utilizados, pelos órgãos e entidades da FUNAI bem como Órgãos Conveniados, estritamente para o fim a que se destinam, no interesse da Administração.

Os usuários são responsáveis pela utilização correta dos recursos colocados à sua disposição, e uso adequado das informações disponibilizadas. Os órgãos e entidades da FUNAI, sob orientação da CTI, devem capacitar seus usuários, para o uso adequado e responsável dos recursos e das informações presentes no Sistema de Telemática.

Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas no âmbito do Sistema de Telemática, ficando os transgressores sujeitos à Lei Penal, Civil e Administrativa, na medida das condutas, dolosa ou culposa, que praticarem.

Não é permitido o acesso, utilização, instalação, manutenção e/ou implantação de qualquer recurso de TI, sem prévio conhecimento e autorização da CGDTI.

Qualquer usuário só poderá utilizar programas de computador licenciados para uso no Sistema de Telemática, desde que constantes da lista de produtos homologados, divulgados pela CGDTI, e exista licença de uso disponível. O responsável pela CTI poderá suprir a falta da lista de produtos homologados, mediante informação, ao interessado, acerca da condição do produto a ser utilizado. A instalação dos programas e sistemas homologados é atribuição da CTI, ou de outro órgão, mediante delegação.

O acesso aos recursos computacionais deverá ocorrer de acordo com o perfil conferido ao usuário.

Não é permitida a instalação de modem em equipamentos que estejam conectados à rede local.

Cada estação de trabalho só poderá ser configurada para utilizar uma sub-rede, não sendo permitida configurá-la para reencaminhar o fluxo de comunicação.

Os serviços de comunicação remota somente são disponibilizados a servidores que exerçam atividades que requeiram freqüente comunicação com a FUNAI em viagens e serviços externos ou a servidores que prestem suporte técnico à infra-estrutura do sistema de telemática, desde que formalmente solicitado à CGDTI.

Os usuários poderão:

Criar, transmitir, distribuir, disponibilizar e armazenar documentos por intermédio do Sistema de Telemática e da Internet, desde que respeite as leis e regulamentações, notadamente, aquelas referentes a: crimes informáticos, ética, decência, pornografia envolvendo crianças, honra e imagem de pessoas ou empresas, vida privada e intimidade.

Copiar documentos e/ou programas de computador objetivando salvaguardá-los, respeitada a legislação que rege a salvaguarda de dados, informações, documentos e materiais sigilosos no âmbito da Administração Pública Federal, exigindo-se autorização para aqueles protegidos pelos direitos autorais, inclusive: músicas, textos, documentos digitalizados e qualquer conteúdo encontrado em jornais, periódicos, livros ou quaisquer outras fontes protegidas por direitos autorais.

Acessar recursos computacionais que estejam em conformidade com o perfil da atividade desempenhada pelo usuário na Instituição;

Comunicar e trocar dados de interesse da administração pública;

Os usuários não devem compartilhar pastas em seus equipamentos, exceto aqueles criados em servidor para esse fim.

A CTI disponibilizará uma área comum para disponibilização temporária de arquivo.

A CTI poderá instituir limites à utilização de recursos telemáticos de modo a resguardar a integridade e a disponibilidade dos ativos de informação.

PROCEDIMENTOS E RESPONSABILIDADES OPERACIONAIS

Os usuários devem estar cientes das regras e normas de uso dos sistemas de telemática, evitando, desse modo, procedimentos que prejudiquem ou impeçam outras pessoas de terem acesso a esses recursos ou de usá-los de acordo com o que é determinado.

Os usuários não podem, deliberadamente, sobrecarregar os recursos de TI.

Cabe ao usuário e a CTI zelarem pelo funcionamento adequado do sistema de telemática

CORREIO ELETRÔNICO

16.1 Ao ler e-mail o usuário deve prestar especial atenção em relação aos remetentes que não conhece ou a mensagens cujo assunto lhe pareça repetido. Os anexos devem ser verificados por um antivírus, mesmo sendo de remetentes conhecidos, tais procedimentos apenas visam à integridade da rede da FUNAI, bem como a privacidade do usuário.

16.2 A disponibilização do serviço de correio eletrônico visa à troca de mensagens, contendo assuntos pertinentes às atividades da FUNAI e no interesse da administração.

16.3 As caixas postais do correio eletrônico são de propriedade da FUNAI, passíveis de monitoração e auditoria pela CTI.

16.4 Usuários que não sejam servidores da FUNAI, a critério do responsável por contrato ou atividade, poderão acessar o serviço de correio eletrônico, nos termos dessa Norma, enquanto perdurar o vínculo com a FUNAI.

16.5 O acesso ao correio eletrônico se dá pelo conjunto Identificação do Usuário e Senha, que é pessoal e intransferível, ou por outra modalidade que vier a ser formalmente instituída.

16.6 As unidades da FUNAI devem promover, junto aos seus usuários, o incentivo ao uso do serviço de correio eletrônico, no desempenho de suas atividades funcionais, objetivando a racionalização do trabalho e o aumento da produtividade, por meio da facilitação da troca de informações e do intercâmbio de idéias.

16.7 As solicitações de novas caixas postais deverão ser encaminhadas à CTI, pela chefia imediata ou superior com os respectivos dados cadastrais.

16.8 Toda unidade administrativa instituída formalmente no organograma da FUNAI poderá possuir, no mínimo, uma caixa postal e dois ou mais usuários responsáveis pela sua administração e manipulação diária, sendo um deles o chefe ou responsável pelas respectivas áreas.

16.9 Quando da solicitação e habilitação de uso do serviço de correio eletrônico, para unidades administrativas, grupos de trabalho e outros usuários despersonalizados, deverá ser identificada junto ao administrador do serviço a pessoa responsável pela sua utilização, bem como o substituto eventual.

16.10 As mensagens deverão ser redigidas de forma clara, devendo conter o grau de formalidade compatível com o destinatário e o assunto tratado, conforme Manual de Redação da Presidência da República.

16.11 Recomenda-se que a transmissão de mensagens e dados sigilosos, por meio da rede e/ou correio eletrônico, sejam cifradas com algoritmos fortes e chaves com tamanho compatível com o grau de sigilo.

16.12 A FUNAI adotará oportunamente um cliente de correspondência institucional único.

16.13 A CTI poderá limitar o número de destinatários externos e internos.

16.14 Os demais usuários que, no interesse do trabalho, necessitarem enviar mensagens com número superior designado de destinatários, devem solicitar essa facilidade, justificando sua necessidade, que a CTI apreciará e decidirá em única instância sobre o pleito.

16.15 A caixa postal sem movimentação por um período igual ou superior a 06 (seis) meses será bloqueada, automaticamente, pela Administração do Correio Eletrônico.

16.16 Os usuários só poderão participar de listas de discussão relacionadas, exclusivamente, ao interesse do trabalho.

16.17 São atribuições dos usuários:

16.17.1 Gerenciar contatos, mensagens, arquivos e anexos contidos nas caixas postais;

16.17.2 Utilizar o correio eletrônico institucional para os objetivos e funções próprios e inerentes às suas atribuições funcionais;

16.17.3 Respeitar a capacidade de armazenamento, no servidor, destinada às caixas postais sob sua responsabilidade;

16.17.4 Negar acesso de terceiros ao correio eletrônico através de sua senha;

16.17.5 Atualizar seus dados cadastrais utilizando os meios disponíveis;

16.17.6 Notificar a CTI e sua chefia imediata ou superior, quando do recebimento de mensagens que contrariem o disposto nesta Norma.

16.18 Para efeito desta Norma, consideram-se usos indevidos do correio eletrônico:

16.18.1 Acessar indevidamente ou sem autorização caixas postais de terceiros, sendo punível a tentativa;

16.18.2 Enviar de informações sensíveis, classificadas ou proprietárias, inclusive senhas, para pessoas ou organizações não autorizadas;

16.18.3 Enviar e armazenar:

a) material pornográfico, ilegal ou não ético, comercial pessoal, de propaganda, mensagens do tipo corrente, entretenimento e "spam" (envio de mensagem não solicitada, para um grande número de pessoas);

b) mensagens que sejam ofensivas ou ainda afetar de forma negativa a imagem do Governo Federal ou da FUNAI;

c) mensagens contendo códigos maliciosos ou qualquer forma de rotinas de programação prejudiciais ou danosas;

d) mensagens contendo calúnia, injúria e difamação;

e) listas de endereços eletrônicos dos usuários do correio eletrônico da FUNAI, com objetivo contrário ao interesse do serviço;

f) material protegido por leis de propriedade intelectual;

g) material de natureza político-partidária ou sindical, que promova candidatos para cargos públicos eletivos, clubes, associações e sindicatos;

h) programas de computador que não sejam destinados ao desempenho das funções regimentais ou que possam ser considerados nocivos ao ambiente de rede da FUNAI; e

i) outros, a critério da CTI.

16.19 Para utilizar o serviço de correio eletrônico institucional, o usuário deve tomar conhecimento, por meio eletrônico ou impresso, de termo de responsabilidade e manutenção de sigilo, além de concordar expressamente com os termos desta Norma;

16.20 Caberá à unidade local de recursos humanos informar a CTI o desligamento ou afastamento definitivo de servidores e estagiários, para que a mesma providencie a desativação da caixa postal.

16.21 Caberá a unidade de modernização administrativa da FUNAI, informar a CTI as alterações das abreviaturas e nomenclaturas dos órgãos internos da FUNAI.

16.22 Caberá à chefia imediata ou superior comunicar a CTI o desligamento de prestadores de serviços terceirizados, temporários e estagiários sob sua responsabilidade para a desativação definitiva da caixa postal.

UTILIZAÇÃO DE INTERNET

O acesso à Internet tem por finalidade a intercâmbio e obtenção de informações relativas às atividades desenvolvidas na FUNAI.

Aos usuários internos da FUNAI não é permitida a transferência anônima de arquivos, e a utilização de comunicações interativas (mensagens instantâneas e bate papo) e de terminais virtuais não homologados.

Não é permitido o estabelecimento de conexão direta, originária da Internet, com destino à rede interna da FUNAI.

Não é permitida a inscrição em sítios de comunicação interativa (bate-papo) ou grupos de discussão (fóruns e listas de discussão) sem a devida autorização.

O download de programas ou arquivos de entretenimento, como por exemplo jogos, músicas ou fotografias, não pode ser efetuado através da ligação Internet da FUNAI. Da mesma forma o uso de jogos contra oponentes na Internet é proibido.

O conteúdo de todas as páginas da Internet visitadas deverá ser condizente com os interesses e a política da FUNAI.

Usuários com acesso à Internet não podem efetuar upload (envio) de qualquer software licenciado ou de dados de propriedade da FUNAI, sem expressa autorização do gerente responsável pelo software ou pelos dados.

PROTEÇÃO CONTRA SOFTWARE MALICIOSO

Nenhum usuário pode utilizar os recursos computacionais para deliberadamente propagar qualquer tipo de código malicioso.

Deve ser feita verificação, antes do uso, da existência de vírus em qualquer arquivo em meio magnético de origem desconhecida ou não autorizada.

ACESSOS, OPERAÇÕES E AÇÕES PROIBIDAS AOS USUÁRIOS

Realizar conexões com qualquer outra organização sem a prévia análise e autorização da área de CGDTI.

Tentar interferir, indevidamente ou sem autorização, em um serviço, sobrecarregá-lo ou, ainda, desativá-lo, inclusive aderir a ataques de negação de serviços internos ou externos.

Fornecer informações, a terceiros, sobre usuários ou serviços disponibilizados no Sistema de Telemática, sem autorização expressa da autoridade competente.

Introduzir no Sistema de Telemática recursos particulares sem autorização da CTI.

Revelar códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves públicas ou privadas etc) ou permitir o uso por terceiros de recursos autorizados por intermédio desses códigos.

Divulgar ou mercanciar produtos, itens ou serviços a partir de qualquer recurso de TI.

Modificar cabeçalho de qualquer dos protocolos que formam o TCP/IP (Transfer Control Protocol/Intenet Protocol) ou alterar registro de evento do sistema de telemática.

Acessar sem autorização dados, sistemas, redes, incluindo qualquer tentativa de investigar, examinar, testar vulnerabilidades ou dispositivo da rede.

Violar medida de segurança ou de autenticação, sem autorização expressa da autoridade competente.

Utilizar-se da Internet para acessar sites ou serviços que possam vir a degradar o link de conexão tais como: ouvir música ou rádio através de sites, conexões a sites de bate-papo e programas de mensagens instantâneas (MIRC, ICQ, MSN, SKYPE e outros).

Utilizar infra-estrutura ou serviços não homologados pela CTI.

Prover meio de acesso à Internet que não seja por intermédio da CTI.

Prover meio de acesso remoto que não seja os oferecidos pela CTI.

Prover conexão com rede externa que não seja homologado pela CTI.

Essas restrições não se aplicam à investigação policial e/ou processo judicial.

NOTIFICAÇÃO DE INCIDENTES DE SEGURANÇA

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.

São exemplos de incidentes de segurança:

- tentativas de ganhar acesso não autorizado a sistemas ou dados;
- ataques de negação de serviço;
- uso ou acesso não autorizado a um sistema;
- modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do proprietário ou gestor do sistema;
- desrespeito à Política de Segurança da Informação.

Os incidentes devem ser reportados o mais rapidamente possível ao superior hierárquico ou a CTI.

Os incidentes de segurança devem ser notificados através do envio de um e-mail para o endereço seguranca@funai.gov.br com as seguintes informações:

Identificação do usuário:

a) nome;
b) telefone;
c) lotação;
d) cargo ou função;

Dados do incidente:

a) data e horário da ocorrência ou dos logs indicando o fuso horário utilizado;
b) endereço IP ou nome da máquina que sofreu ataque;
c) endereço IP ou nome da máquina que efetuou o ataque;
d) descrição do ataque;
e) outras informações relevantes ao tratamento deste incidente;
f) logs relacionados ao incidente.

Os dados fornecidos serão tratados com sigilo inerente ao tratamento de incidentes de segurança da informação.

NOTIFICAÇÃO DE FALHAS DE SEGURANÇA

Quaisquer fragilidades ou ameaças, ocorridas ou suspeitas, na segurança de sistemas ou de serviços devem ser registradas e notificadas o mais rápido possível aos superiores e à Equipe de Segurança da Informação.

Os usuários, para sua própria proteção, não podem, sob nenhuma circunstância, tentar averiguar uma fragilidade suspeita, pois a investigação de uma fragilidade pode ser interpretada como potencial uso impróprio do sistema ou atentar possíveis suspeitas.

NOTIFICAÇÃO DE MAU FUNCIONAMENTO DE APLICATIVO

Qualquer detecção de mau funcionamento de aplicativo deve ser registrada e notificada o mais rápido possível aos superiores.

Os usuários não devem tentar remover o problema do aplicativo, a menos que sejam autorizados.

DIREITOS DE PROPRIEDADE INTELECTUAL

O uso dos recursos computacionais (hardware e software) deve ser de acordo com leis de propriedade intelectual, com as de direitos autorais, patentes ou marcas registradas. A violação do direito autoral pode levar a uma ação legal envolvendo processos criminais.

Qualquer software não oficial encontrado em equipamentos da FUNAI é de inteira responsabilidade de seu usuário, ficando o mesmo sujeito a penas e sanções legais impostas pela legislação em vigor.

O Sistema de Telemática deverá ser utilizado sem violação dos direitos de propriedade intelectual de qualquer pessoa ou empresa, como marcas e patentes, nome comercial, segredo empresarial, domínio na Internet, desenho industrial ou qualquer outro material, que não tenha autorização expressa do autor ou proprietário dos direitos, relativo à obra artística, científica ou literária.

PROPRIEDADE DA INFORMAÇÃO

Os documentos produzidos por intermédio do Sistema de Telemática são de propriedade da FUNAI. De igual modo, os programas desenvolvidos por agentes públicos para a FUNAI. Ressalvadas as hipóteses em haja licença de uso diversa.

Qualquer informação pertinente aos dados da FUNAI só poderá ser divulgada mediante autorização do gestor da informação.

A FUNAI reserva-se o direito de apagar arquivos armazenados em seus computadores desde que contenham dados não condizentes com esta Norma de Segurança de Informação.

SUSPENSÃO DE PRIVILÉGIOS INDIVIDUAIS

Privilégios especiais não são incorporados permanentemente aos direitos dos usuários.

A CTI pode suspender todos os privilégios de determinado usuário em relação ao uso de redes e computadores sob sua responsabilidade, por razões ligadas à segurança física, ou por razões disciplinares ou relacionadas à Segurança da Informação e ao bem-estar dos outros usuários.

O acesso será prontamente restabelecido quando a Segurança da Informação e o bem-estar puderem ser assegurados.

APURAÇÃO DE RESPONSABILIDADES

A ocorrência de furto, extravio ou defeito de equipamento, decorrente de dolo ou culpa ensejará apuração de responsabilidade nos termos previstos em norma própria, cabendo, no caso de prejuízos ao Erário, a quem seja imputada a responsabilidade, ressarcir aos cofres públicos.

Havendo fundadas razões do cometimento de transgressões à presente norma, quem dela tomar ciência poderá comunicar a superior hierárquico e os dirigentes de qualquer unidade deverão, de ofício, apurar ou fazer com que se apure a irregularidade.

DISPOSIÇÕES FINAIS

As dúvidas e os casos omissos em relação a esta Norma serão resolvidos pela autoridade do Senhor Presidente da FUNAI, conforme o caso requerer.

Esta Norma entra em vigor na data de sua publicação.

FORMULÁRIO DE CREDENCIAMENTO PARA ACESSO À REDE CORPORATIVA DE COMUNICAÇÃO E DADOS

CREDENCIAMENTO PARA ACESSO À REDE CORPORATIVA DE COMUNICAÇÃO E DADOS

Usuário			
Nome Completo:	***Situação Funcional:*** ☐ **Quadro** ☐ **Somente DAS** ☐ **Cont. Temporário** ☐ **Estagiário** ☐ **Outros**		**Matrícula:**
Identificação na Rede:	**Lotação:**	**Grupo de Trabalho:**	
E-mail: @funai.gov.br	**Ramal:**		

Técnico da Rede	
Nome:	**Assinatura:**

Autorização do Chefe do Setor	
Nome:	**Assinatura e Carimbo:**

Termo de Responsabilidade

Declaro que nesta data, um técnico da Gerência da Rede Coorporativa de Comunicação e Dados do Departamento de Informática, me cadastrou como usuário dos servidores de rede existentes, tendo recebido orientações básicas de utilização da rede, ficando-me atribuída a senha individual e sigilosa, tornando-me ciente das disposições referente à segurança da Rede e, comprometendo-me a:

1. Manter absoluta cautela quando da exibição de dados em tela ou impressora, bem como na gravação em meios eletrônicos, a fim que deles não venham tomar ciência pessoas não autorizadas.
2. Não me ausentar da estação de trabalho sem encerrar a sessão (LOGOUT) do uso da Rede, garantindo a impossibilidade de uso indevido por pessoas não autorizadas.
3. Acompanhar a impressão e recolher os documentos cuja impressão tenha solicitado.
4. Utilizar a Internet e Correio Eletrônico (se for o caso) somente para fins de interesse da FUNAI.
5. Informar à Coordenação de Tecnologia da Informação quando houver mudança de setor de lotação, bem como o desligamento da FUNAI.

Responder, em todas as instâncias devidas, pelas conseqüências decorrentes das ações ou omissões de minha parte que possam por em risco ou comprometer a exclusividade de conhecimento da minha senha ou das transações em que esteja habilitado, especialmente pela introdução de vírus na Rede.

Autenticação		
Assinatura do Usuário:	**Data:**	**Hora:**

TERMO DE RESPONSABILIDADE E MANUTENÇAO DE SIGILO

Identificação do Usuário			
CPF:		Usuário nível:	(Preenchido pela CTI)
Nome:			
Setor:			
Órgão:		Telefone:	

FULANO DE TAL, portador do documento de identidade nº _____, expedido pela [entidade], CPF nº _____, em consonância com o disposto nos normativos que tratam do uso dos recursos de tecnologia da informação e comunicação da Fundação Nacional do Índio, dos quais tenho conhecimento, declaro-me ciente de que o uso indevido, desautorizado ou para qualquer outro fim que não seja estritamente o interesse do serviço, de quaisquer recursos disponibilizados, seja acesso a rede de computadores, à Internet, conta de correio eletrônico, divulgação de senha pessoal etc., ensejará apuração de responsabilidades, cabendo a quem imputada a culpa as penalidades administrativas porventura cabíveis.

Comprometo-me a manter sigilo sobre dados, processos, informações, documentos, materiais e instalações que venha a ter acesso ou conhecimento, em razão das atividades profissionais a serem realizadas, nos termos da Lei ou por determinação expressa de superior hierárquico a fim de evitar que deles venham a tomar ciência pessoas não autorizadas.

Neste ato, o signatário declara que leu e entendeu a Política de Segurança da Informação e a Norma de Uso Aceitável dos Recursos de Tecnologia da Informação; que se compromete a zelar pelos recursos de tecnologia da informação e comunicação colocadas à sua disposição; responsabilizando-se a indenizar e assumir os danos que venham a ser causados ao erário, conforme preceitua o artigo 122 da Lei nº 8.112, de 11 de dezembro de 1990, pelo uso indevido dos recursos de tecnologia da informação e comunicação da FUNAI, inclusive por qualquer reclamação de calúnia, difamação, injúria, violação de direitos de reserva e infração de propriedade intelectual ou outros direitos, arcando com todos os ônus decorrentes (obrigações, perdas, custos, despesas, honorários advocatícios etc.).

E por estar de acordo, firma o presente Termo na presença das testemunhas abaixo mencionadas.

Autorizado por: Em ___/___/_____ _____ Chefia Imediata Usuário	De acordo: Em ___/___/_____ _____ Usuário	Credenciado por: Em ___/___/_____ _____ CTI – Coordenação de Tecnologia da Informação

* Em conformidade com "Boas Práticas em Segurança da Informação – TCU (2003)"