Uso de Recursos Computacionais

DIRETRIZES E NORMAS

MUNDO **VIRTUAL,** SEGURANÇA **REAL.**

Dispõe sobre as orientações, as regras, as responsabilidades e as proibições mandatórias associadas à disciplina e a utilização dos recursos computacionais, disponibilizados e mantidos pelo INCA para uso corporativo, o que inclui os equipamentos, as instalações físicas, os softwares e os serviços que direta ou indiretamente estão relacionados ao processamento, ao armazenamento e à transmissão digital de dados (acesso à rede interna de comunicação de dados, acesso à Internet, acesso ao e-mail institucional e o acesso aos sistemas corporativos de informação), as regras para disciplinar o acesso aos meios de armazenamento de dados, aos meios de impressão e o uso de dispositivos móveis portáteis.

CONTROLE DE DISTRIBUIÇÃO

Quanto ao grau de confidencialidade, este documento é classificado como **PÚBLICO.**

CONTROLE DE REVISÕES

Data	Revisão	Natureza da Alteração	Autor
02/10/2009	Original	Elaboração	Área de Recursos Tecnológicos - STI
31/03/2015	1ª Revisão	Atualização	Área de Recursos Tecnológicos - STI
20/05/2016	2ª Revisão	Atualização	Área de Recursos Tecnológicos - STI
10/07/2017	3ª Revisão	Atualização	Área de Gov. e Inovação em TIC - STI

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES

1.1 Apresentação

Esta NORMA, estabelecida na forma de Anexo, para observância e aplicação, elaborada pelo **SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO,** é considerada parte integrante e inseparável da **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA e, eventualmente, no que couber, dos seus DOCUMENTOS COMPLEMENTARES integrantes, uma vez que os complementa, embora com ênfase em outros aspectos.

Esta NORMA utiliza, na forma de Anexo, no que couber, o disposto no **GLOSSÁRIO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.

1.2 Convenções deste Documento

Para os fins de uniformidade dos procedimentos contidos nesta NORMA, considera-se o disposto na **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.

1.3 Campo de Aplicação

Esta NORMA aplica-se, de forma mandatória e em sentido lato, exclusivamente no âmbito do INCA, incluindo todas as suas Unidades Administrativas e Hospitalares, para todo o PÚBLICO-ALVO desta NORMA.

1.4 Objetivo

Esta NORMA objetiva estabelecer diretrizes e normas que se aplicam de forma mandatória para todos os usuários que utilizam os RECURSOS COMPUTACIONAIS, disponibilizados pelo INCA, visando assegurar os simultâneos acesso e proteção da informação com ênfase seus principais aspectos de segurança (confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade, legalidade, conformidade, privacidade e confiabilidade), levando em consideração as vulnerabilidades exploráveis por ameaças e agressões com risco de impacto negativo; e tendo ênfase seletiva nos aspectos das seguranças física, lógica e de recursos humanos.

1.5 Público-alvo

Para os fins de uniformidade dos procedimentos contidos nesta NORMA, considera-se o disposto na **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.

1.6 Vigência

Esta NORMA tem prazo de validade indeterminado, portanto, sua vigência se estenderá desde sua publicação, gerando efeitos imediatos, até a edição de outro marco normativo que motive sua atualização ou a revogação.

1.7 Publicação

Esta NORMA será publicada e disponibilizada, pelo **COMITÊ ESTRATÉGICO E GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES (CEGTIC)**, após aprovação, para acesso ou *download*, a qualquer tempo, a todos os usuários, de forma permanente nos canais de comunicação internos do INCA (inclusive na Intranet do INCA), disposta de maneira que seu conteúdo possa ser consultado a qualquer momento, sem prejuízo dos pertinentes meios oficiais de publicação aplicáveis, e no D.O.U.

1.8 Conceitos e Definições

Para os fins de uniformidade dos procedimentos contidos nesta NORMA, considera-se os conceitos e definições que constam do **GLOSSÁRIO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.

1.9 Referências Legais e Normativas

Esta NORMA obedecerá aos princípios constitucionais, administrativos e ao arcabouço legislativo vigente que rege a Administração Pública Federal.

As referências legais e normativas utilizadas como base para a elaboração desta NORMA são, principalmente, as seguintes:

1.9.1 Boas Práticas

NBR/ISO/IEC 27001:2006 - Gestão de Segurança da Informação, que dispõe sobre os requisitos para Sistemas de Gestão de Segurança da Informação.

1.9.2 Normas Complementares (NC)

NC nº 07/IN01/DSIC/GSIPR, de 15 de Julho de 2014, que dispõe sobre as Diretrizes para a **Implementação de Controles de Acesso** relativos à Segurança da Informação e Comunicações.

NC nº 12/IN01/DSIC/GSIPR, de 15 de Julho de 2014, que dispõe sobre as Diretrizes e orientações básicas para o **uso de Dispositivos Móveis** nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

2 USO DOS RECURSOS COMPUTACIONAIS

A Segurança da Informação será implementada no nível de aplicação e no nível de infraestrutura cobrindo toda a área de TI.

O uso de RECURSOS COMPUTACIONAIS, disponibilizados pelo INCA, será regido por um conjunto de diretrizes gerias e, conforme o caso, outras específicas, ambas dispostas neste DOCUMENTO, visando estabelecer os critérios de manuseio, de prevenção e de responsabilidades sobre o uso destes, sendo aplicadas de forma mandatória a todos os colaboradores que os utilizem.

A utilização de RECURSOS COMPUTACIONAIS **NÃO** disponibilizados pelo INCA, portanto, particulares ou de terceiros na rede do INCA deve observar os seguintes pontos:

- Para acesso restrito à Internet: é permitido, respeitando-se as regras definidas na **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.
- Para acesso a dados: é proibido. Se necessário, exceções devem ser autorizadas pelo gerente da área demandante, desde que sejam adotados os mecanismos de segurança homologados pelo INCA.

2.1 Tipos de Recursos Computacionais

São considerados RECURSOS COMPUTACIONAIS os equipamentos (*hardware*), as instalações físicas, os programas de computador (*softwares*), os serviços que direta ou indiretamente estão relacionados ao processamento, ao armazenamento e à transmissão digital de dados, bem como, qualquer dado acessível por meio desses equipamentos ou programas de computador, agregado ou não na forma de ESTAÇÃO DE TRABALHO, que integre a qualquer título o patrimônio do INCA como ativo tecnológico informático, tangível ou intangível, ou que, mesmo não o integrando, seja utilizado nele ou para ele, o que inclui, dentre outros similares:

- Computadores de mesa (*desktops*) de qualquer espécie.

- Computadores servidores de rede de qualquer espécie.
- Computadores portáteis de colo (*laptops*) de qualquer espécie.
- Computadores portáteis de mão de qualquer espécie (inclusive os smartphones)
- Terminais de autoatendimento (quiosques).
- Dispositivos periféricos de qualquer espécie (inclusive para acessibilidade por parte de portadores de necessidades especiais) destinados a conexão em computadores (tais como monitores, teclados, *mouses*, caixas de som, fones de ouvido, microfones, leitoras, hubs, gravadoras, HDs externos, *pen drives*, cartões de memória, *chips*, câmeras, *scanners*, impressoras, multifuncionais, cartuchos, *toners*, *tokens*, smartcards, HSM (*hardware security module)*, equipamentos de biometria, equipamentos de videoconferência, projetores, *touch boards*, mesas digitalizadoras, *modems*, roteadores, cabos, adaptadores, estabilizadores, filtros e *no-breaks*).
- Equipamentos que compõem o *Datacenter*.
- Equipamentos de redes internas (Intranet), bem como a rede de comunicação de dados que as interliga e as liga a redes externas (*Internet*), com ou sem fio (via onda infravermelha, *Wi-Fi*, *Bluetooth*, outras espécies de ondas de rádio etc.).
- Programas de computador de qualquer espécie (tais como aplicativos e sistemas);
- Endereços e correios eletrônicos (tais como *sites*, *e-mails*, calendários, agendas, catálogos de contatos e gerenciadores de tarefas).
- Ferramentas eletrônicas de comunicação de dados de qualquer espécie.
- Dados de qualquer espécie armazenados em computadores, dispositivos periféricos e outros equipamentos, bem como em CDs, DVDs e outras mídias, dispostos ou não em banco de dados (tais como arquivos e certificados digitais).
- Sistemas de Segurança.

- Bancos de Dados.
- Sistemas operacionais e sistemas legados[1].

2.2 Diretrizes Gerais

É de competência da **GERÊNCIA DE RECURSOS TECNOLÓGICOS** a gestão (especificação, instalação, administração e manutenção) dos RECURSOS COMPUTACIONAIS do INCA, os quais cumprirão todas as leis aplicáveis, incluindo, entre outras, leis de privacidade, leis de propriedade intelectual, leis antisspam, exigências regulatórias e orientações governamentais.

A **ÁREA DE SEGURANÇA DA INFORMAÇÃO**, poderá bloquear o acesso a *sites* externos, em função de:

- Conteúdo incompatível com as atividades profissionais.
- Desrespeito à legislação nacional.
- Risco à Segurança da Informação na rede de computadores do INCA.

2.2.1 Recursos Computacionais Passíveis de Utilização

Para integrarem ou deixarem de integrar a qualquer título o patrimônio do INCA, bem como para terem expandida sua utilização, os RECURSOS COMPUTACIONAIS deverão se submeter previamente, conforme o caso, a:

- Contratação.
- Teste, avaliação e homologação, pela **GERÊNCIA DE RECURSOS TECNOLÓGICOS**, com ênfase nos requisitos de segurança da informação, principalmente o nível de impacto negativo.
- Autorização ou aprovação, pelo responsável pela STI.

[1] Sistema legado é o termo utilizado em referência aos sistemas computacionais de uma organização que fornecem serviços essenciais. No caso específicos do INCA, por exemplo, Alert e Abosolute.

Deverão ser utilizados no INCA ou para ele:

- Os RECURSOS COMPUTACIONAIS que integrem a qualquer título seu patrimônio.
- Excepcionalmente, os RECURSOS COMPUTACIONAIS que não integrem seu patrimônio, inclusive na linha do BYOD (*Bring Your Own Device*, em português "traga seu próprio dispositivo") ou da computação em nuvem (*cloud computing*), principalmente em situações de contingência, desde que previamente submetidos, conforme o caso, às operações descritas no item anterior.

Se for o caso, os RECURSOS COMPUTACIONAIS deverão ser agregados na forma de ESTAÇÕES DE TRABALHO conforme um padrão comum, para a grande maioria das unidades e usuários, que exerce atividades sem peculiaridades técnicas relevantes, ou conforme determinados padrões especiais (tais como para administradores, técnicos, pesquisadores, estagiários, empregados de "terceirizados", dentre outros), com máximo ou mínimo privilégio, para as unidades e usuários que exercem atividades com peculiaridades técnicas relevantes, ou para acessibilidade por parte de portadores de necessidades especiais.

A ESTAÇÃO DE TRABALHO deverá ser individual e intransferível, sendo possível, no entanto, o regime de expressa substituição eventual.

A impressora poderá ser compartilhada, enquanto baixo o risco de impacto negativo.

Todos os componentes das ESTAÇÕES DE TRABALHO deverão ter uma configuração previamente estabelecida, pela **GERÊNCIA DE RECURSOS TECNOLÓGICOS**, principalmente quanto aos processos técnicos passíveis de automação, ressalvada a possibilidade de ajustes de menor proporção por parte do próprio usuário.

As finalidades, conteúdos e práticas dos RECURSOS COMPUTACIONAIS não poderão comprometer o desempenho técnico dos próprios recursos, bem como o desempenho funcional de seu usuário, se for o caso.

Os RECURSOS COMPUTACIONAIS que integrem o patrimônio do INCA poderão ser utilizados, excepcionalmente, fora de suas instalações, independentemente de ser ou não em teletrabalho, principalmente em situações de contingência, desde que previamente submetidos, conforme o caso, às operações descritas no item “a”, acima descrito.

Se vierem a estar fora da vigilância de seu proprietário, possuidor ou detentor, inclusive em trânsito, independentemente de estar sendo utilizado em teletrabalho, bem como se vierem a deixar de ser utilizados, o computador, bem como todas as específicas formas de acesso lógico, deverão se submeter a desligamento, bloqueio ou saída (*sign-out*, *logoff* ou *logout*), preferencialmente de modo automático.

É recomendável que o computador portátil disponha de mecanismos remotos de localização via rede ou GPS - *global positioning system* (ou seja, sistema de posicionamento global), bem como de desligamento, bloqueios, saída (*logoff* ou *logout*), cópia de segurança (*backup*) e apagamento, preferencialmente de modo automático.

Qualquer conduta deverá ter sua relevância avaliada independentemente de ser comissiva ou omissiva, dolosa ou culposa, consumada ou tentada.

2.2.2 Controle de Utilização dos Recursos Computacionais

Poderá ser preventivo, detectivo ou reativo, dando-se prévia, simultânea ou posteriormente, priorizando-se o primeiro.

Deverá ser previamente avisado e agendado, exceto se for alto o risco de impacto negativo, constatado pela unidade responsável pela TI.

Poderá ser ordinário ou extraordinário, gerando relatório.

Poderão ser utilizados os seguintes mecanismos de controle:

- Efetuação de registro e manutenção preferencialmente durante o prazo para aplicar ou buscar a aplicação da penalidade para o tipo de infração mais grave.
- Rastreamento, varredura ou verificação periódica (tal como levantamento físico e inventário).
- Bloqueio de conteúdo.
- Limitação de prática.
- Restrição de propriedades (tais como tipo e tamanho).
- Submissão a quarentena ou suspensão.
- Remoção ou interrupção.
- Inspeção periódica.

Os mecanismos de controle, sempre atualizados, deverão ser ativados de modo automatizado (tal como mediante a utilização de software ANTIVÍRUS e ANTIMALWARE), sem a possibilidade de desativação, ressalvada a possibilidade de revisão do resultado dessa automatização, a pedido ou de ofício e resguardada a inviolabilidade do sigilo dos dados classificados em qualquer grau de sigilo, conforme a Lei nº 12.527, de 2011.

De modo complementar, os arquivos armazenados em dispositivos apropriados, quando abertos pela primeira vez, deverão se submeter a utilização de software ANTIVÍRUS.

Aplicam-se subsidiariamente os mecanismos de controle de todos os recursos materiais.

Qualquer incidente que, envolvendo utilização de RECURSOS COMPUTACIONAIS, aparentemente tenha relevante risco de impacto negativo, deverá ser imediatamente reportado, por

quem tomar conhecimento, ou mesmo de modo automatizado, ao respectivo Gestor Negócio e, daí, à **ÀREA DE RECURSOS TECNOLÓGICOS**, para os devidos fins.

2.2.3 Conteúdos dos Recursos Computacionais

Os RECURSOS COMPUTACIONAIS, com destaque para os computadores, impressoras, *softwares* e arquivos:

- Deverão ser aplicados e tratar de informações necessárias ou úteis ao serviço prestado no INCA.
- Também poderão tratar de informações que, embora não sejam necessárias ou úteis ao serviço prestado no INCA, sejam concernentes, dentre outros temas, a educação, saúde, trabalho, comunicação, cidadania, serviços públicos ou de interesse público, governo e poderes estatais.

2.2.4 Responsabilidades do Usuário do Credenciado

- Desligar a ESTAÇÃO DE TRABALHO ou computador portátil corretamente (diariamente) ao final do expediente, seguindo os procedimentos do sistema operacional.
- As ESTAÇÕES DE TRABALHO ou computadores portáteis devem ser ligadas somente em pontos elétricos estabilizados, evitando-se que sejam ligados em conjunto com outros equipamentos elétricos que não sejam RECURSOS COMPUTACIONAIS.
- Armazenar os arquivos com informações corporativas nos SERVIDORES DE ARQUIVOS disponibilizados na REDE INTERNA DE COMUNICAÇÃO DE DADOS. Deve-se evitar o armazenamento nas ESTAÇÕES DE TRABALHO.
- Evitar realizar conversas em locais públicos ou sem a reserva adequada sobre assuntos sensíveis da Instituição, restringindo-se a tratá-los somente em locais que ofereçam a proteção adequada.

- Colaborar ativamente na solução de problemas e no aprimoramento dos processos de Segurança da Informação.

2.2.5 Responsabilidades dos Administradores E-mail Institucional

- Administrar as políticas e procedimentos relativos aos serviços de *e-mail* institucional e assegurar o cumprimento de leis e normas aplicáveis.
- Verificar periodicamente o desempenho e a integridade do sistema de *e-mail* institucional.
- Estabelecer procedimentos e rotinas de manutenção de contas de *e-mail* institucional.

2.3 Diretrizes Específicas

2.3.1 Arquivos de Dados e Informações

São os dados e informações que devem ser protegidos contra acessos não autorizados, bem como, a respetiva motivação para tanto:

- Arquivos de Código Fonte dos *Softwares* - O acesso não autorizado ao código fonte dos *softwares* pode ser usado para alterar suas funções e a lógica do programa ou para identificar vulnerabilidades não percebidas pelos desenvolvedores.
- Arquivos de Dados - Bases de dados, arquivos ou transações de bancos de dados devem ser protegidas para evitar que os dados sejam apagados ou alterados sem autorização, como, por exemplo, arquivos com a configuração do sistema, dados da folha de pagamento, dados estratégicos da empresa.
- Arquivos de Senha - A falta de proteção adequada aos arquivos que armazenam as senhas pode comprometer todo o sistema, pois uma pessoa não autorizada, ao obter identificador (ID) e senha de um usuário privilegiado, pode, intencionalmente, causar danos ao sistema.

Essa pessoa dificilmente será barrada por qualquer controle de segurança instalado, já que se faz passar por um usuário autorizado.

- Arquivos de Log (Registro) - Os arquivos de log são usados para registrar ações dos usuários, constituindo-se em ótimas fontes de informação para auditorias futuras. Os logs registram quem acessou os RECURSOS COMPUTACIONAIS, aplicativos, arquivos de dados e utilitários, quando foi feito o acesso e que tipo de operações foram efetuadas. Um invasor ou usuário não autorizado pode tentar acessar o sistema, apagar ou alterar dados, acessar aplicativos, alterar a configuração do sistema operacional para facilitar futuras invasões, e depois alterar os arquivos de *log* para que suas ações não possam ser identificadas. Dessa forma, o administrador do sistema não ficará sabendo que houve uma invasão.
- Utilitários e Sistema Operacional - O acesso aos utilitários (como editores, compiladores, *softwares* de manutenção, monitoração e diagnóstico) deve ser restrito, já que essas ferramentas podem ser usadas para alterar aplicativos, arquivos de dados e de configuração do sistema operacional, por exemplo. O sistema operacional é sempre um alvo bastante visado, pois sua configuração é o ponto-chave de todo o esquema de segurança. A fragilidade do sistema operacional compromete a segurança de todo o conjunto de aplicativos, utilitários e arquivos.

2.3.2 Cópia de Segurança e Guarda de Dados na Rede

Faça regularmente cópias de segurança de seus documentos e dados armazenados em seu computador de trabalho, a fim de 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 revistas, livros ou quaisquer outras fontes protegidas por direitos autorais.

Mantenha registros das cópias de segurança.

Guarde as cópias de segurança em local seguro e distinto daquele onde se encontra a informação original.

2.3.3 Bloqueio de Sites

A **ÀREA DE RECURSOS TECNOLÓGICOS** reserva-se o direito de bloquear, a seu critério e sem aviso prévio, o acesso a todos os *sites* de *Internet* que julgar inadequados, impróprios, prejudiciais ou não necessários ao desenvolvimento das atividades diárias de trabalho dos colaboradores dentro do INCA.

Caso o usuário necessite de acesso a algum site que esteja bloqueado, deverá solicitar a liberação mediante o documento de **SOLICITAÇÃO DE SERVIÇO CORPORATIVO DE TI**. Este documento deverá passar pela análise da **ÀREA DE RECURSOS TECNOLÓGICOS** e em seguida encaminhado para autorização da Direção da TI.

2.3.4 Estações de Trabalho

As ESTAÇÕES DE TRABALHO fornecidas possuirão configurações de *hardware* e *software* padronizadas pela **GERÊNCIA DE RECURSOS TECNOLÓGICOS**, de acordo com a necessidade de utilização dos usuários e serão lacradas a fim de evitar modificações não autorizadas.

Nas ESTAÇÕES DE TRABALHO, somente deverão ser instalados *softwares* homologados e licenciados pela **GERÊNCIA DE RECURSOS TECNOLÓGICOS** e necessários para a execução das atividades dos usuários.

É vedado à **GERÊNCIA DE RECURSOS TECNOLÓGICOS** conceder aos usuários privilégios de administrador local nas ESTAÇÕES DE TRABALHO, salvo em casos excepcionais, mediante justificativa do titular da unidade e parecer da **GERÊNCIA DE RECURSOS TECNOLÓGICOS**.

Os titulares das unidades poderão solicitar a instalação de *softwares* complementares nas ESTAÇÕES DE TRABALHO, cabendo à **GERÊNCIA DE RECURSOS TECNOLÓGICOS** analisar a possibilidade de atendimento.

As atualizações e correções de segurança de sistemas operacionais deverão ser aplicadas pela **GERÊNCIA DE RECURSOS TECNOLÓGICOS** após a validação em ambiente de homologação, assim que disponibilizadas pelo fabricante.

As ESTAÇÕES DE TRABALHO possuirão *software* ANTIVÍRUS instalado, ativado e permanentemente atualizado.

Os usuários deverão bloquear a ESTAÇÕES DE TRABALHO sempre que se afastarem dela, sendo necessária a digitação da senha de acesso para a liberação da área de trabalho.

As ESTAÇÕES DE TRABALHO terão bloqueio de tela automático, ativado por tempo de inatividade habilitado, com intervalo de bloqueio fixado em cinco minutos desde a última atividade detectada.

Quando possível, os recursos de hibernação e de suspensão serão habilitados nas ESTAÇÕES DE TRABALHO, de forma a economizar energia elétrica. Caso não seja possível habilitar tais recursos numa estação, ela deve ser desligada ao final do expediente, salvo recomendação expressa da **GERÊNCIA DE RECURSOS TECNOLÓGICOS** a esse respeito.

O usuário deve informar à **GERÊNCIA DE RECURSOS TECNOLÓGICOS** quando identificar violação da integridade física do equipamento por ele utilizado.

A solicitação de instalação ou substituição de ESTAÇÕES DE TRABALHO deverá ser feita através do HELPDESK, após os trâmites administrativos necessários.

Após a instalação do equipamento solicitado, se necessário, o HELPDESK deverá informar ao solicitante as instruções para a utilização do recurso.

2.4 Serviços Corporativos

Os SERVIÇOS CORPORATIVOS são disponibilizados pela STI aos USUÁRIOS CREDENCIADOS com base nos RECURSOS COMPUTACIONAIS.

2.4.1 Tipos de Serviços Corporativos

São considerados SERVIÇOS CORPORATIVOS:

- Rede Interna de Comunicação de Dados
- Acesso à *Internet*
- *E-mail* Institucional
- SISTEMAS CORPORATIVOS DE INFORMAÇÃO
- Meios de Armazenamento de Dados
- Meios e Impressão
- DISPOSITIVOS MÓVEIS Portáteis
- Datacenter

2.4.2 Acesso aos Serviços Corporativos

Os SERVIÇOS CORPORATIVOS só podem ser usados por USUÁRIOS CREDENCIADOS, respeitando o perfil de acesso de cada atribuição de trabalho.

Todos os USUÁRIOS INTERESSADOS (todo o PÚLICO-ALVO deste DOCUMENTO), têm direito de acesso aos SERVIÇOS CORPORATIVOS, condicionado ao prévio credenciamento, observadas as condições dispostas neste DOCUMENTO, na **NSIC 01 – CONCESSÃO DE CONTA DE ACESSO PESSOAL** e na **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES**.

O acesso do USUÁRIO CREDENCIADO aos SERVIÇOS CORPORATIVOS será feito por controles de acesso físicos ou lógicos (conforme o caso), com objetivo de proteger equipamentos, *softwares* e arquivos de dados contra perda, modificação ou divulgação não autorizada.

Todos os USUÁRIOS CREDENCIADOS deverão estar cientes de que o uso indevido dos SERVIÇOS CORPORATIVOS caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar ao INCA e/ou a terceiros.

O acesso remoto, aos SERVIÇOS CORPORATIVOS e informações corporativas do INCA, a partir da *Internet* deve observar os seguintes pontos:

- Deve ser realizado em horário de expediente. Se necessário, exceções devem ser autorizadas pelo gerente da área demandante.
- No período de férias, licença ou afastamento é proibido, sem exceção.
- Acesso ao *e-mail* institucional disponibilizado pelo INCA é permitido e automaticamente criptografado.
- Acesso a dados é permitido, desde que seja autorizado pelo gerente da área demandante e com criptografia.
- Deve ser feito a partir de computadores fornecidos pelo INCA. O acesso a partir de computadores particulares somente pode ser feito quando adotados os mecanismos de segurança homologados pelo INCA. O acesso a partir de computadores públicos (fornecidos por *LAN Houses, Cybercafés*, etc.) ou de terceiros não são permitidos.
- Se necessário, pode ser realizado a partir de locais públicos (*shoppings centers*, hotéis, aeroportos, dentre outros). Os usuários devem atentar para as responsabilidades que assumem quanto à segurança dos computadores utilizados e ter cautela com a exposição de informações sensíveis expostas em tela.

- O acesso remoto deve ser imediatamente revogado ao término do vínculo de trabalho com o INCA. Neste caso, os equipamentos de propriedade do INCA deverão ser devolvidos antes da homologação do desligamento.

2.4.3 Uso dos Serviços Corporativos

2.4.3.1 Obrigações de Uso

Ao utilizar os SERVIÇOS CORPORATIVOS, o USUÁRIO CREDENCIADO deve obrigatoriamente:

- Utilizá-los baseado no bom senso e de maneira honesta e profissional, inclusive NÂO publicando conteúdo inapropriado, impreciso ou questionável.
- Utilizá-los 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, relativos à obra artística, científica ou literária.
- Manter as informações de caráter reservado, sigiloso ou confidencial protegidas.
- Ter comportamento decoroso e de acordo com os preceitos legais.
- Comunicar prontamente a **ÁREA DE RECURSO TECNOLÓGICOS** quaisquer eventos de quebra de segurança, tais como recebimento de informação sigilosa por engano, adulteração de informação, roubo de informação, ou ainda, ameaças ou ataques virtuais (conforme disposto no documento **CSIC - CARTILHA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES**).

2.4.3.2 Finalidades de Uso

Os SERVIÇOS CORPORATIVOS devem ser utilizados em atividades imediatamente relacionadas ao serviço prestado no INCA, por lhe serem necessárias, e poderão ser utilizados em atividades mediatamente relacionadas ao serviço prestado no INCA, por lhe serem úteis.

Os SERVIÇOS CORPORATIVOS são disponibilizados para uso corporativo com o propósito único de garantir o desempenho das atividades profissionais de trabalho (para os fins a que se destinam e no interesse da administração, não podendo ser interpretados como de uso pessoal).

Instituições e pessoas não vinculadas ao INCA poderão ter autorização para utilizar os SERVIÇOS CORPORATIVOS, desde que respeitadas às diretrizes de uso estabelecidas especificamente para esse fim.

É considerada imprópria a utilização dos SERVIÇOS CORPORATIVOS para propósitos não profissionais (particulares), não autorizados ou quaisquer outras atividades que contrariem os objetivos institucionais do INCA ou às leis vigentes. Os usuários e visitantes que tomarem conhecimento dessa prática devem levá-la ao conhecimento de seu superior imediato para que sejam aplicadas as ações disciplinares cabíveis.

Todos os SERVIÇOS CORPORATIVOS devem ser protegidos e conservados, segundo as diretrizes descritas neste DOCUMENTO e demais regulamentações em vigor, de forma a preservar os seus componentes internos, externos e acessórios.

2.4.3.3 Monitoramento de Uso

O INCA, por meio da **ÁREA DE RECURSOS TECNOLÓGICOS**, poderá monitorar, auditar e registrar todo o uso dos SERVIÇOS CORPORATIVOS, visando garantir a disponibilidade e a segurança das informações utilizadas e/ou a apuração de um ato administrativo.

2.4.4 Diretrizes Específicas

2.4.4.1 Rede Interna de Comunicação de Dados

É de competência da **GERÊNCIA DE RECURSOS TECNOLÓGICOS** disponibilizar, manter e gerenciar o serviço de acesso à REDE INTERNA DE COMUNICAÇÃO DE DADOS no INCA.

O acesso à REDE INTERNA DE COMUNICAÇÃO DE DADOS, só pode ser realizado por um USUÁRIO CREDENCIADO, utilizando sua CONTA DE ACESSO pessoal válida.

Todo o tráfego na REDE INTERNA DE COMUNICAÇÃO DE DADOS é considerado confidencial. Não sendo permitido desenvolver, usar ou divulgar dispositivos ou sistemas que possibilitem a violação de dados na REDE INTERNA DE COMUNICAÇÃO DE DADOS.

Todos os acessos à REDE INTERNA DE COMUNICAÇÃO DE DADOS devem ser alvo de controle e monitoração com o objetivo de verificar possíveis irregularidades a este DOCUMENTO, e seu uso deve ser somente para fins corporativos relacionados às atividades do colaborador dentro da instituição.

Todo acesso a um serviço da REDE INTERNA DE COMUNICAÇÃO DE DADOS não explicitamente autorizado deve ser bloqueado ou desabilitado.

2.4.4.2 Acesso à Internet

Sob o aspecto de proteção e integridade dos SISTEMAS CORPORATIVOS DE INFORMAÇÃO, a *Internet* é classificada como conexão de alto risco. O USUÁRIO CREDENCIADO deve estar ciente, portanto, da peculiaridade da navegação na *Internet*, antes de acessá-la e de utilizar os seus recursos.

Considerando que o uso da *Internet*, no âmbito do INCA, 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.

Todos os USUÁRIOS CREDENCIADOS, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do INCA, mantendo uma conduta profissional.

É de competência da **GERÊNCIA DE RECURSOS TECNOLÓGICOS** disponibilizar, manter e gerenciar o serviço de acesso à *Internet*.

O acesso à *Internet*, só pode ser realizado por um USUÁRIO CREDENCIADO, utilizando sua CONTA DE ACESSO pessoal válida.

O INCA possui mecanismos de autenticação, que determinam a titularidade de todos os acessos à *Internet* feitos por seus USUÁRIOS CREDENCIADOS.

Todos os acessos à *Internet* devem ser utilizados exclusivamente:

- Para fins diretos e complementares às atividades profissionais exercidas no INCA.
- Para o enriquecimento intelectual de seus colaboradores.
- Como ferramenta para busca por informações que venham contribuir para o desenvolvimento de seus trabalhos.

O acesso à *Internet* jamais deve ser utilizado para a realização de trabalhos de terceiros ou de atividades paralelas.

A utilização do acesso à *Internet* para fins pessoais, como a consulta a movimento bancário ou acesso a *e-mail* pessoal, deve ser realizada no horário do almoço ou fora horário de expediente.

Todos os acessos à *Internet* serão alvo de controle e monitoração com o objetivo de verificar possíveis irregularidades a **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA. A simples abertura de um *site* da *Internet* desconhecido ou de origem duvidosa - pode ser o suficiente para a ocorrência de ameaças digitais ou virtuais (conforme exposto, no item “Segurança da Informação”, da **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA), permitindo

que o atacante tome o controle do computador da vítima — método muito usado pelos invasores de computadores.

O USUÁRIO CREDENCIADO é o único responsável por decidir se deseja acessar ou utilizar *sites* de terceiros disponibilizados na *Internet*.

2.4.4.3 E-mail Institucional (Correio Eletrônico Corporativo)

É de competência da **GERÊNCIA DE RECURSOS TECNOLÓGICOS** disponibilizar, manter e gerenciar o serviço de *e-mail* institucional.

O acesso ao *e-mail* Institucional, só pode ser realizado por um USUÁRIO CREDENCIADO, utilizando sua CONTA DE ACESSO pessoal válida.

O serviço de *e-mail* institucional disponibilizado pelo INCA constitui recurso disponibilizado na REDE INTERNA DE COMUNICAÇÃO DE DADOS para aumentar a agilidade, segurança e economia da comunicação oficial e informal. O *e-mail* institucional constitui bem do INCA e, portanto, passível de auditoria.

Toda a CONTA DE ACESSO terá uma titularidade, determinando o USUÁRIO CREDENCIADO como único responsável e responsável direto do sobre a sua utilização.

As mensagens de e-mail institucional sempre devem incluir assinatura com o seguinte formato:

- Nome do colaborador
- Gerência ou departamento
- Nome da empresa
- Telefone(s)
- *e-mail* Institucional

As mensagens de *e-mail* institucional sempre devem incluir um Aviso Legal (normalmente colocado no rodapé das mensagens) produzido pelo **SERVIÇO DE COMUNICAÇÃO SOCIAL** e aprovado pela Diretoria Executiva.

É recomendada a utilização de técnicas de criptografia e assinatura digital para proteger a confidencialidade e integridade dos *e-mails* quando do tramite de informações classificadas, seguindo sempre a legislação vigente que trata deste assunto.

As mensagens emitidas através do *e-mail* institucional são elementos de formação da imagem institucional e, como tal, devem merecer o mesmo tratamento da correspondência impressa.

Toda informação veiculada eletronicamente será alvo de controle e monitoração, e seu uso deve ser tão somente para fins corporativos relacionados às atividades do colaborador dentro da instituição. A simples abertura de um anexo de *e-mail*, pode instalar um *software* com Código Malicioso, permitindo que o atacante tome o controle do computador da vítima — método muito usado pelos invasores de computadores.

São requisitos técnicos se aplicam à entrega de *e-mail* institucional, através da REDE INTERNA DE COMUNICAÇÃO DE DADOS do INCA:

- Reclamações enviadas por usuários do INCA devem ser usadas como base para a recusa de conexões de qualquer sistema de *e-mail*.
- O servidor de *e-mail* institucional:
  - Não aceitará conexões oriundas de sistemas inseguros. Sendo que estes incluem *open relays*[2], *open proxies*[3] ou qualquer outro sistema em que seja constatada a disponibilidade de ser utilizado de forma indevida ou insegura.

[2] Open Relay são servidores de em-mail que processam um e-mail onde o remetente e o destinatário não são usuários do servidor em questão. Estes servidores de em-mail constituem uma ameaça à rede de computadores, pois são utilizados pelos spammers para enviar seus e-mails indiscriminadamente.

[3] Open Proxy é um servidor proxy que é acessível por qualquer usuário da Internet. Normalmente, este servidor só deve estar acessível aos usuários que estão dentro do grupo de rede da empresa.

- Não aceitará conexões de sistemas que se encontram configurados com IP's.
- Adotará mecanismos de combate à *Spam*, tais como: Lista de Bloqueio[4], Filtro de Conteúdo[5], *Greylisting*[6], *Sender Policy Framework* (SPF)[7], *DomainKeys Identified Mail* (DKIM)[8], dentre outros.
- Não entregará *e-mails* suspeitos de estiverem utilizando-se de técnicas para burlar filtros *anti-spam* tais como *URL*'s encodadas em hexadecimal (ex: http://%6d%6e%3f/), arquivos do tipo texto ou html encodados em Base64.
- Possuirá um sistema de análise de fluxo de *e-mails* que pode rejeitar conexões de servidores que possuam um comportamento suspeito de *SPAM*.

- O servidor de *e-mail* institucional poderá rejeitar conexões de:
  - Endereços IP's que não estejam de acordo com as recomendações da RFC[9] 1912 (*Common DNS Operational and Configuration Errors*), em relação às configurações de DNS-reverso (exigência de uma entrada PTR válida e autoritativa).
  - Servidores de rede cuja lista de destinatários gere de forma consistente mais do que 10% de erros. (Ex: Mais de 10% da lista de *e-mails* é destinada a usuários que não existem em nosso sistema).

4 Lista de Bloqueio o mais antigo mecanismo de combate ao spam. Estas listas são bases de dados de endereços IP que tenham sido identificados como possível fonte de spam, segundo os critérios da entidade que mantém a lista. As listas normalmente funcionam através de consultas DNS às bases de dados.

5 Filtro de Conteúdo é técnica de bloqueio de spam que se baseia na análise do conteúdo da mensagem. Em geral, são filtros baseados no reconhecimento de padrões do conteúdo que buscam identificar se o e-mail pode conter um vírus ou se tem características comuns aos spams.

6 Greylisting (em português Lista Cinza) implementada em um servidor de e-mail, fará com que o servidor de e-mail recuse, temporariamente, qualquer e-mail de um emissor desconhecido e espere por sua retransmissão. Caso o emissor seja um servidor de e-mail legítimo e não um software de spam, tentará enviar a mensagem novamente em um intervalo de tempo aceito pelo servidor de destino.

7 Sender Policy Framework (SPF) é uma tecnologia para combater a falsificação de endereços de retorno dos emails (return-path).

8 DomainKeys Identified Mail (DKIM) é um mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas.

9 RFC (acrónimo em inglês de Request for Comments), é uma série de documentos que contém notas técnicas e organizacionais sobre a Internet. Eles cobrem muitos aspectos da rede de computadores, incluindo protocolos, procedimentos, programas e conceitos.

- Remetentes que são incapazes de aceitar ao menos 90% das mensagens de erro/retorno (*mailer-daemon*[10], mensagens de erro/falha) destinadas ao seu sistema.

- O servidor de *e-mail* institucional poderá rejeitar:
  - Mensagens quando o endereço IP de origem da conexão não for definido como válido de acordo com sua entrada SPF, para todos os domínios[11] que publicam o registro SPF.
  - O envio de mensagens quando as mensagens com arquivos anexados (texto e anexo) possuírem tamanho superior a 10 *Mbytes* (para e-mails com 2 anexos ou mais, vale a somatória dos anexos).

2.4.4.4 Sistemas Corporativos de Informação

É de competência da **GERÊNCIA DE DESENVOLVIMENTO DE SISTEMAS** disponibilizar, manter e gerenciar o serviço de acesso a cada SISTEMA CORPORATIVO DE INFORMAÇÃO.

A instalação (quando for requerida uma instalação no computador do usuário) de cada SISTEMA CORPORATIVO DE INFORMAÇÃO é atribuição da **GERÊNCIA DE RECURSOS TECNOLÓGICOS**, podendo ser suportada (conforme o caso) pela **GERÊNCIA DE DESENVOLVIMENTO DE SISTEMAS**.

O acesso a cada SISTEMA CORPORATIVO DE INFORMAÇÃO, só pode ser realizado por um USUÁRIO CREDENCIADO, utilizando sua CONTA DE ACESSO pessoal válida.

O INCA, caso considere prudente ou necessário, poderá (sem aviso prévio):

- Limitar a utilização dos SERVIÇOS CORPORATIVOS, parcial ou integralmente, para um ou mais usuários, inclusive o número de suas conexões e a sua capacidade.

[10] Mailer-daemon é um software de servidor de e-mail que é responsável pela entrega dos e-mails. O recebimento de um mailer-daemon, pode indicar um problema com o endereço de e-mail do destinatário ou do servidor ou um endereço de e-mail incorreto.

[11] Domínio é o endereço de um site na internet. Por exemplo: www.inca.gov.br

- Restringir, suspender ou encerrar uma CONTA DE ACESSO, se comprovar que o USUÁRIO CREDENCIADO violou as diretrizes de segurança da **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA, a lei ou que utilizou os SERVIÇOS CORPORATIVOS de forma indevida (por exemplo, violação de quaisquer indicações de o que você deve e não deve fazer).

2.4.4.5 Meios de Armazenamento de Dados

Todos os arquivos contendo informações corporativas deverão ser armazenados nos SERVIDORES DE ARQUIVOS do INCA, visando garantir a integridade, disponibilidade e confidencialidade das informações.

É de competência da **GERÊNCIA DE RECURSOS TECNOLÓGICOS** disponibilizar, manter e gerenciar tais SERVIDORES na REDE INTERNA DE COMUNICAÇÃO DE DADOS, incluindo a realização de cópias de segurança (*backups*) periódicas e os mecanismos necessários para a proteção das informações armazenadas.

É de competência do USUÁRIO CREDENCIADO armazenar tais arquivos nos SERVIDORES DE ARQUIVOS disponibilizados na REDE INTERNA DE COMUNICAÇÃO DE DADO, devendo evitar o armazenamento nas ESTAÇÕES DE TRABALHO.

Todas as informações corporativas, armazenadas em cada SISTEMA CORPORATIVO DE INFORMAÇÃO, devem ser armazenadas nos SERVIDORES DE DADOS do INCA, visando garantir a integridade, disponibilidade e confidencialidade das informações.

É de competência da **GERÊNCIA DE RECURSOS TECNOLÓGICOS** disponibilizar, manter e gerenciar tais SERVIDORES na REDE INTERNA DE COMUNICAÇÃO DE DADOS, incluindo a realização de cópias de segurança (*backups*) periódicas e os mecanismos necessários para a proteção das informações armazenadas.

Todos os arquivos pessoais deverão ser armazenados nas ESTAÇÕES DE TRABALHO ARQUIVOS do INCA.

A salvaguarda das informações armazenadas nas ESTAÇÕES DE TRABALHO ficará a cargo do USUÁRIO CREDENCIADO, que deverá responsabilizar-se por esses dados e pela realização de cópias de segurança (*backups*) periódicas, antes de manutenções do equipamento.

Os dados deverão ser armazenados, conforme os níveis de acesso, criticidade ou prioridade, em dispositivos:

- Apropriados.
- Com limite de capacidade adequado.
- Preferencialmente internos, inclusive, se for o caso, com segregação ("conteinerização").
- Preferencialmente do INCA.
- Com ou sem criptografia baseada em algoritmo de Estado.

Os dados também poderão ser armazenados, excepcionalmente, conforme os níveis de acesso, criticidade ou prioridade, em dispositivos:

- Externos.
- Particulares, individuais ou compartilháveis.
- Sem criptografia.

Todos os dados armazenados, com destaque para os críticos ou prioritários, deverão ou poderão ter cópias de segurança (backups) providenciadas, periodicamente, por seu proprietário, possuidor ou detentor, conforme o caso.

Em caso de necessidade de recuperação de informações perdidas armazenadas nos servidores do INCA, o usuário deverá abrir chamado junto ao HELPDESK, que irá tomar providências para a recuperação, quando possível, e irá orientá-lo quanto ao acesso aos arquivos.

2.4.4.6 Meios de Impressão

Os dispositivos de impressão disponibilizados pelo INCA são para uso exclusivo em serviço.

Sempre que possível, o compartilhamento de documentos deve ser priorizado, o que evitará o uso desnecessário de insumos ou de cota de impressão.

As impressoras disponibilizadas aos usuários que possibilitarem impressão frente e verso da folha de papel terão esta opção habilitada como modalidade de impressão padrão.

A opção de impressão em um só lado da folha deve ser utilizada apenas na hipótese de extrema necessidade, de forma a evitar o uso desnecessário de recursos.

As impressões em cores devem ser utilizadas apenas em hipótese de extrema necessidade, de forma a evitar o uso desnecessário de recursos.

Em caso de problemas, o HELPDESK deverá ser acionado, excluindo-se os casos mais simples, como reabastecimento de papel, que deverá ser efetuado pelo próprio usuário.

A **GERÊNCIA DE RECURSOS TECNOLÓGICOS** disponibilizará, mensalmente, relatórios demonstrando o quantitativo de impressões de cada unidade, nos quais serão discriminados, pelo menos, os totais de impressão frente e verso, em apenas um lado da folha, em preto e branco e em cores.

A solicitação de instalação de novo dispositivo de impressão deverá ser feita ao HELPDESK.

Após a instalação do dispositivo solicitado, caso aprovado, o HELPDESK deverá informar ao solicitante as instruções para a utilização do recurso, bem como os procedimentos necessários ao seu bom funcionamento, inclusive nas situações comuns do dia a dia, como o desatolamento de papel.

Em nenhuma hipótese o usuário deverá abrir o equipamento mediante a utilização de ferramentas.

2.4.4.7 Dispositivos Móveis

São considerados DISPOSITIVOS MÓVEIS os equipamentos portáteis dotados de capacidade computacional, tais como:

- Notebooks
- -Netbooks
- Smartphones
- Tablets

São considerados DISPOSITIVOS MÓVEIS os dispositivos removíveis de memória para armazenamento, tais como:

- Pendrives
- USB Drives
- HDs Externos (Discos Rígidos Externos)
- Cartões de Memória
- Mídias Regraváveis

É de competência da **GERÊNCIA DE RECURSOS TECNOLÓGICOS**:

- Disponibilizar, manter e gerenciar tais DISPOSITIVOS MÓVEIS.
- Prover sistemas que efetuem o bloqueio de utilização de DISPOSITIVOS MÓVEIS CORPORATIVOS sem autorização, a fim de evitar a fuga de informações corporativas.
- Cadastrar os DISPOSITIVOS MÓVEIS CORPORATIVOS, garantindo sua identificação única, bem como a do usuário responsável pelo uso.
- Implementar os mecanismos de autenticação, autorização e registro de acesso do usuário, bem como do DISPOSITIVO MÓVEL CORPORATIVO às conexões de rede e recursos disponíveis.
    - Caso um Colaborador deseje conectar seu próprio DISPOSITIVO MÓVEL PARTICULAR (desde que seu uso esteja devidamente autorizado pela **GERÊNCIA DE RECURSOS TECNOLÓGICOS**) à REDE INTERNA DE COMUNICAÇÃO DE DADOS do INCA, o mesmo procedimento, descrito no item anterior, deve ser adotado.
    - Caso um Visitante deseje conectar seu próprio DISPOSITIVO MÓVEL (desde que seu uso esteja devidamente autorizado pela **GERÊNCIA DE RECURSOS TECNOLÓGICOS**) à REDE INTERNA DE COMUNICAÇÃO DE DADOS do INCA, o mesmo procedimento, descrito no item anterior, deve ser adotado. A concessão de uso deve estar vinculada à conscientização do usuário sobre as normas internas de uso da rede.
- Adotar mecanismos que garantam a proteção e sigilo dos dados armazenados no DISPOSITIVO MÓVEL CORPORATIVO em casos de extravio, tais como, solução de criptografia de disco.
    - Caso um colaborador deseje utilizar seu próprio DISPOSITIVO MÓVEL PARTICULAR, recomenda-se que seja adotado o mesmo procedimento, descrito no item anterior.
- Aplicam-se, quando pertinentes, aos DISPOSITIVOS MÓVEIS CORPORATIVOS as mesmas regras de utilização das ESTAÇÕES DE TRABALHO.

- O Usuário deverá registrar uma solicitação no HELPDESK quando desejar utilizar, por empréstimo, um DISPOSITIVO MÓVEL CORPORATIVO do INCA dotado de capacidade computacional.
  - O Usuário ao receber um DISPOSITIVO MÓVEL CORPORATIVO torna-se responsável pelo mesmo e, caso ainda não tenha assinado, deve assinar o **TERMO DE RESPONSABILIDADE**.
  - O DISPOSITIVO MÓVEL CORPORATIVO deve ser utilizado única e exclusivamente pelo próprio usuário, assumindo a responsabilidade pelo seu uso e obedecendo às orientações da **GERÊNCIA DE RECURSOS TECNOLÓGICOS**.
  - Este usuário, não deve instalar aplicativos ou recursos não disponibilizados pela **GERÊNCIA DE RECURSOS TECNOLÓGICOS** sem permissão prévia.
  - Na devolução do DISPOSITIVO MÓVEL CORPORATIVO, o usuário deverá retirar todos os arquivos gravados e manipulados durante a utilização, além de todos os objetos pessoais, como CDs.
  - Este DISPOSITIVO MÓVEL CORPORATIVO, sempre que não estiver sendo utilizado, deve ser guardado em local seguro, onde o responsável, por estes, possa garantir que os mesmos não serão utilizados por outras pessoas.
  - Os arquivos armazenados no DISPOSITIVO MÓVEL CORPORATIVO deverão ser, sempre que possível, protegidos por senhas de acesso ou por criptografia.
  - Todos devem realizar periodicamente cópia de segurança (*backup*) dos dados de seu DISPOSITIVO MÓVEL CORPORATIVO. Deverão, também, manter estes *backups* separados de seu dispositivo, ou seja, não carregá-los juntos.
  - Todos devem utilizar senhas de bloqueio automático para seu DISPOSITIVO MÓVEL CORPORATIVO.

- Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da **GERÊNCIA DE RECURSOS TECNOLÓGICOS**.
- O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da **GERÊNCIA DE RECURSOS TECNOLÓGICOS**.
- É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.
- É responsabilidade do colaborador, no caso de furto ou roubo de um DISPOSITIVO MÓVEL CORPORATIVO fornecido pelo INCA, notificar imediatamente seu gestor direto e a **GERÊNCIA DE RECURSOS TECNOLÓGICOS**. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).
- O colaborador deverá estar ciente de que o uso indevido do DISPOSITIVO MÓVEL CORPORATIVO caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar ao INCA e/ou a terceiros.

- O colaborador que desejar utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à REDE INTERNA DE COMUNICAÇÃO DE DADOS do INCA deverá submeter previamente tais equipamentos ao processo de autorização da **GERÊNCIA DE RECURSOS TECNOLÓGICOS**, definirá a quais recursos ou dados corporativos o DISPOSITIVO MÓVEL PARTICULAR terá acesso.
  - É necessária a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário, bem como do dispositivo às conexões de rede e recursos disponíveis.

- É recomendada a adoção de mecanismos que garantam a proteção e sigilo dos dados corporativos armazenados no DISPOSITIVO MÓVEL PARTICULAR em casos de extravio.

- Com relação aos DISPOSITIVOS MÓVEIS CORPORATIVOS ou PARTICULARES removíveis de memória para armazenamento:
  - As informações classificadas somente podem ser armazenadas em DISPOSITIVOS MÓVEIS removíveis que possibilitem a aplicação de controles compatíveis com seu nível de classificação.
  - Devem ser utilizados considerando-se soluções de segurança, de acordo com a **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.

2.4.5 Proibições aos Usuários

É vedado a todos os USUÁRIOS CREDENCIADOS, dentre outros similares:

- Adotar condutas que interfiram na operação normal e adequada dos SERVIÇOS CORPORATIVOS e que adversamente afetem a capacidade de outras pessoas utilizarem esses recursos, bem como condutas que sejam prejudiciais e ofensivas.
- Abrir o gabinete das ESTAÇÕES DE TRABALHO ou computador portátil, modificar qualquer configuração, seja de *hardware* ou *software*, sem autorização prévia da **GERÊNCIA DE RECURSOS TECNOLÓGICOS**. Essas configurações são padronizadas, conforme definições da **GERÊNCIA DE RECURSOS TECNOLÓGICOS**. Havendo a necessidade de alteração destas configurações, a solicitação deve ser encaminhada à **GERÊNCIA DE RECURSOS TECNOLÓGICOS** para análise.
- Desenvolver, gerar, compilar, copiar, coletar, propagar, executar ou tentar introduzir qualquer código fonte de *software* projetado para se auto-replicar, danificar ou de outra

maneira obstruir o acesso ou afetar o desempenho de qualquer computador, da rede de computadores ou de um SISTEMA CORPORATIVO DE INFORMAÇÃO.

- Instalar ou executar *software* de sua propriedade ou de terceiros, sem prévia homologação e autorização da área de TI.
- Introduzir códigos maliciosos nos sistemas de TI.
- Revelar códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves privadas e etc) ou permitir o uso por terceiros de recursos autorizados por intermédio desses códigos.
- Divulgar ou comercializar produtos, itens ou serviços a partir de qualquer recurso dos sistemas de TI.
- Tentar interferir ou interferir, sem autorização, em um SERVIÇO CORPORATIVO, sobrecarregá-lo, interrompê-lo ou, ainda, desativá-lo, inclusive aderir ou cooperar com ataques de negação de serviços (*DoS - Denial of Service*) internos ou externos.
- Alterar registro de evento dos sistemas de TI.
- Modificar cabeçalho de qualquer protocolo de comunicação de dados.
- Obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas de TI.
- Monitorar ou interceptar o tráfego de dados nos sistemas de TI, sem a autorização de autoridade competente.
- Violar medida de segurança ou de autenticação, sem autorização de autoridade competente.
- Fornecer informações a terceiros, sobre usuários ou serviços disponibilizados nos sistemas de TI, exceto os de natureza pública ou mediante autorização de autoridade competente.
- Fornecer dados classificados de acordo com a legislação vigente, sem autorização de autoridade competente.

- Armazenar ou usar de jogos nos computadores do INCA.
- Armazenar ou usar sistema informacional dos órgãos e instituições da Administração Pública Federal, sem prévia autorização.
- Usar os SERVIÇOS CORPORATIVOS para fins pessoais, incluindo entre estes o comércio, venda de produtos ou engajamento em atividades comerciais de qualquer natureza.
- Uso de aplicativos não homologados nos recursos informacionais do INCA.

É vedado a todos os USUÁRIOS CREDENCIADOS usar os SERVIÇOS CORPORATIVOS, dentre outros similares:

- De modo ilícito, imoral, abusivo, inconfiável, inseguro, anônimo ou com alto risco de impacto negativo, **GERÊNCIA DE RECURSOS TECNOLÓGICOS**, inclusive para tratar informações.
- Para violar direitos de propriedade de informação ou mecanismos de Segurança da Informação.
- Para interceptação, invasão, subtração, adulteração, prejuízo ou destruição de SERVIÇOS CORPORATIVOS, mediante violação ou desativação de mecanismos de controle de segurança da informação (*hacking*).
- Para proliferação de CÓDIGOS MALICIOSOS (*malwares*) ou exploradores de vulnerabilidades (*exploits*) de qualquer espécie (tais como vírus, *worms*, "Cavalos de Tróia" e *keyloggers*).
- Para obtenção de informações mediante fraude ("*phishing*"), ou de qualquer outra espécie de vantagem mediante fraude, num contexto de "engenharia social".
- Para difusão de informações de qualquer espécie (texto, imagem estática, imagem dinâmica ou som) não solicitadas (SPAM), principalmente com caráter comercial, político, partidário, eleitoral etc.
- Para difusão de boatos.

- Para constranger, assediar, ofender, caluniar, ameaçar, causar prejuízos ou transtornos a qualquer pessoa física ou jurídica.
- Para armazenar, transmitir ou compartilhar arquivos pessoais ou não relacionados às suas atividades nos recursos corporativos da REDE INTERNA DE COMUNICAÇÃO DE DADOS, tais como vídeos, fotos, músicas, jogos, apresentações e apostilas.
- Para tratar de informações concernentes a temas desnecessárias ou inúteis ao serviço prestado no INCA, o que inclui, dentre outros similares:
  - Conteúdos que sejam objeto de crime, contravenção, improbidade administrativa, infração disciplinar ou ética, ato jurídico ilícito ou qualquer outra espécie de infração.
  - Pornografia.
  - Violência.
  - Assuntos pessoais, inclusive relacionamentos.
  - Jogos e qualquer outra espécie de entretenimento.

2.4.5.1 Acesso à Internet

É vedado a todos os Usuários, dentre outros similares:

- Divulgar e/ou compartilhar indevidamente informações da área administrativa do INCA em listas de discussão, sites ou comunidades de relacionamento, salas de batepapo ou *chat*, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na *Internet*.
- Usar, instalar, copiar ou a distribuir *softwares*, sem autorização prévia, que tenham direitos autorais, marca registrada ou patente na *Internet*.
- Acessar *sites* que tiverem conteúdo de pedofilia, racismo ou qualquer outro assunto contrário à lei que, eventualmente, não esteja bloqueado no sistema de proteção do INCA.

- Efetuar *upload* (subida) de qualquer *software* licenciado ao INCA ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo *software* ou pelos dados.
- Acessar e utilizar *sites* ou efetuar *download* (baixa) e utilizar *softwares* que apresentam alto consumo de banda de *Internet*, tais como compartilhamento de arquivos *peer-to-peer* (*Kazaa*, *BitTorrent* e afins), telefonia ou conversação instantânea (MSN, SKYPE, ICQ e afins), serviços de streaming (TV, rádios on-line, canais de broadcast e afins), serviços de multimídia (permitem o *download* de arquivos MP3 ou multimídia) e jogos de computador ou de qualquer outro mecanismo que venha promover serviço semelhante, existentes e que venham a existir.
- Eventuais concessões podem ocorrer, em regime de exceção, desde que sejam cumpridas as seguintes regras:
  - É de competência do servidor público (responsável pelo departamento ao qual o USUÁRIO INTERESSADO estiver vinculado) solicitar formalmente uma CONCESSÃO ESPECIAL para um USUÁRIO INTERESSADO, através de formulário específico (**SOLICITAÇÃO DE SERVIÇO CORPORATIVO DE TI**) assinado, estando à solicitação condicionada ao respectivo deferimento.
  - O USUÁRIO INTERESSADO deve comprovar que um ou mais dos serviços de *softwares* supracitados tenham natureza intrínseca às suas atividades de profissionais no INCA.
  - É de competência da **ÁREA DE RECURSOS TECNOLÓGICOS**, analisar e aprovar a referida solicitação, que poderá ser indeferida sempre que for julgada improcedente.
  - É de competência da Direção da TI a, posterior, autorização de deferimento da referida solicitação, bem como, o respectivo indeferimento sempre que for julgada improcedente.

- Em caso de deferimento da solicitação, é de competência da **ÁREA DE RECURSOS TECNÓLOGICOS** a criação de grupos de segurança para viabilizar essa CONCESSÃO ESPECIAL.
- A referida CONCESSÃO ESPECIAL, que se dá em regime de exceção, poderá ser revogada a qualquer tempo, por solicitação do gestor ou da **ÀREA DE SEGURANÇA DA INFORMAÇÃO**.

- Acessar a sites de proxy.
- Utilizar outros meios de conexão à *Internet* ou de outro tipo de rede a partir de ESTAÇÕES DE TRABALHO do INCA, seja através de modems 3G ou 4G ou de qualquer outro tipo existente ou que venha a ser criado, salvo mediante expressa autorização da **GERÊNCIA DE RECURSOS TECNOLÓGICOS**.

2.4.5.2 Serviços Corporativos

Com relação aos SERVIÇOS CORPORATIVOS, é vedado a todos os Usuários, dentre outros similares:

- Monitorar a disponibilidade, o desempenho ou a funcionalidade dos Serviços para quaisquer fins competitivos.
- Envolver-se em atividades de “enquadramento,” “espelhamento,” ou de outro modo simular a aparência ou a função dos Serviços.
- Acessar os Serviços, utilizando ou tentando utilizar a CONTA DE ACESSO de outra pessoa.
- Acessar os Serviços, exceto por meio das interfaces expressamente fornecidas pelo INCA, tais como seus aplicativos.
- Burlar ou tentar burlar qualquer recurso de segurança dos Serviços.

- Divulgar informações de caráter reservado, sigiloso ou confidencial, para outras pessoas ou para o INCA.
- Difamar, Assediar, abusar, chocar, intimidar, prejudicar ou violar os direitos de outras pessoas.
- Ameaçar de violência ou de danos materiais, ou ainda, atacar as pessoas por causa de sua raça, etnia, nacionalidade, sexo, orientação sexual, filiação política ou religiosa, ou condição médica ou física.
- Agir de forma ilegal, fraudulenta, difamatória, abusiva, obscena, discriminatória ou de outro modo questionável.
- Copiar ou utilizar informações, conteúdo ou dados de outras pessoas disponíveis nos Serviços (exceto com autorização expressa).
- Violar direitos de propriedade intelectual de terceiros, inclusive patentes, marcas comerciais, segredos comerciais, direitos autorais ou outros direitos de propriedade.
- Acessar, usar, guardar, hospedar ou encaminhar material impróprio, não ético, discriminatório, malicioso, obsceno ou ilegal, por intermédio de quaisquer dos meios recursos de comunicações disponibilizados pelo INCA.
- Utilizar *software*, dispositivos, *scripts* robôs ou outros meios ou processos, manuais ou automatizados, para acessar, capturar, sondar ou espionar secretamente outrem, os Serviços ou quaisquer dados ou informações a eles relacionadas.
- Interferir no funcionamento, interromper ou colocar uma carga não razoável nos Serviços, Servidores da REDE INTERNA DE COMUNICAÇÃO DE DADOS do INCA, por meio de qualquer método ilícito ou não autorizado (por exemplo, *spam*, ataque de negação de serviços (*DoS - Denial of Service*) internos ou externos, vírus, algoritmos de jogos).
- Infectar outros computadores ou Servidores da REDE INTERNA DE COMUNICAÇÃO DE DADOS do INCA ou de terceiros, intencionalmente com vírus de *software*, com Códigos Maliciosos ou

com outros *softwares* que podem destruir ou interromper o funcionamento de seus dispositivos ou dados.

- Alugar, arrendar, emprestar, negociar, vender/revender acesso aos Serviços ou a quaisquer informações ou dados a eles relacionados.

2.4.5.3 Rede Interna de Comunicação de Dados

É vedado a todos os Usuários, dentre outros similares:

- Desenvolver, usar ou divulgar dispositivos ou sistemas que possibilitem a violação de dados na REDE INTERNA DE COMUNICAÇÃO DE DADOS.
- Acessar, copiar, alterar ou remover arquivos de terceiros sem autorização explícita, ressalvados casos especiais protegidos por lei ou regulamento próprio.

- É vedado ao Usuário usar os SERVIÇOS CORPORATIVOS, dentre outros similares, para tentar:
  - Obter acesso não autorizado, tais como, tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor de rede, da própria REDE INTERNA DE COMUNICAÇÃO DE DADOS ou de contas de REDE INTERNA DE COMUNICAÇÃO DE DADOS, inclusive de terceiros. Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a um servidor de rede ou conta de REDE INTERNA DE COMUNICAÇÃO DE DADOS cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes.
  - Interferir nos serviços de qualquer outro usuário, servidor de rede ou da própria REDE INTERNA DE COMUNICAÇÃO DE DADOS. Isso inclui ataques, tentativas de congestionar a REDE INTERNA DE COMUNICAÇÃO DE DADOS, sobrecarregar ou invadir um servidor de rede ou, ainda o computador de outro usuário.

- É vedado ao Usuário usar os SERVIÇOS CORPORATIVOS para armazenar, transmitir, divulgar ou disponibilizar qualquer conteúdo, dentre outros similares, que:
  - Contenha vírus ou qualquer outro código, arquivo ou programa de computador com o propósito de interromper, destruir ou limitar a funcionalidade de qualquer software, hardware ou equipamento de telecomunicações.
  - Seja ilegal, ofensivo à honra, que invada à privacidade de terceiros, que seja vulgar, obsceno, pornográfico, preconceituoso, racista, neonazista, antissemita ou qualquer outro que venha a atentar contra a integridade moral de terceiros ou grupos da sociedade.
  - Viole qualquer patente, marca, segredo de negócio, direito autoral ou qualquer outro direito da Instituição.

2.4.5.4 E-mail Institucional (Correio Eletrônico Corporativo)

Todo o tráfego de *e-mail* institucional é considerado confidencial. Não sendo permitido desenvolver, usar ou divulgar dispositivos ou sistemas que possibilitem a violação de qualquer conteúdo do *e-mail* institucional, do próprio ou de terceiros.

O uso do *e-mail* institucional deve ser extremamente profissional. Não podendo ser utilizado para fins pessoais.

E-mails não corporativos não podem ser usados para envio ou recebimento de mensagens relacionadas ao trabalho, exceto em caso de indisponibilidade do *e-mail* institucional, formalmente notificada pela Gerência de TI, e para mensagens urgentes.

É vedado a todos os Usuários usar os serviços de *e-Mail* Institucional, dentre outros similares, para:

- Produzir, manusear, transmitir ou divulgar conteúdo que:

- Contrarie o disposto na legislação vigente, a moral e os bons costumes e a ordem pública.
- Caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos pela lei ou por este DOCUMENTO, lesivos aos direitos e interesses do INCA, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (*hardware* e *software*), bem como os documentos e arquivos de qualquer tipo, do usuário.
- Seja de caráter calunioso, difamatório, injurioso, falso, ofensivo, humilhante, degradante, infame, ofensivo, violento, ameaçador, pornográfico, vulgar, obsceno, imoral, grosseiro, inapropriado, impreciso ou questionável, dentre outros.
- Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas.
- Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do INCA.
- Atente contra a honra.
- Faça apologia, indução, iniciação ou incitação ao crime, à violência, às drogas, às práticas cruéis contra animais, ao nazismo, à exploração sexual, à pedofilia, à pornografia ou a qualquer ilegalidade, ou ainda, que desrespeite a privacidade alheia.
- Faça apologia, indução, iniciação ou incitação ao preconceito ou a discriminação quanto à origem, raça, etnia, sexo, orientação sexual, cor, idade, crença religiosa ou qualquer outra forma de discriminação.
- Possa ser interpretado como de caráter preconceituoso ou discriminatório a pessoa ou grupo de pessoas.

- Contenha conteúdo, linguagem, imagem ou material considerado pornográfico ou atividades ilegais incluindo menores de 18 anos (segundo o artigo 241 do Estatuto da Criança e do Adolescente).
- Contenha linguagem ou imagem grosseira ou obscena.
- Contenha vírus de *software* ou qualquer outro Código Malicioso.
- Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança.
- Perturbe, abuse ou envie *spam* ou outras comunicações não desejadas a outras pessoas (tais como, lixo eletrônico, "correntes", esquemas de "pirâmides", fraudes, *phishing* ou outras práticas semelhantes de aliciamento não autorizado).
- Defenda ou estimule às práticas de bulimia e/ou anorexia.
- Tenha fins políticos locais ou do país (propaganda política).
- Contenha material que viole qualquer lei municipal, estadual ou federal vigente do Brasil.
- Contenha informação relativa à pirataria de *software*.
- Vise obter acesso não autorizado a outro computador, servidor de rede ou rede.
- Vise interromper um serviço, Servidores da REDE INTERNA DE COMUNICAÇÃO DE DADOS do INCA, por meio de qualquer método ilícito ou não autorizado.
- Vise burlar qualquer sistema de segurança.
- Vise vigiar secretamente ou assediar outro usuário.
- Vise acessar informações confidenciais sem explícita autorização do proprietário.

- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa.
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.
- Inclua imagens criptografadas ou de qualquer forma mascaradas.
- Caracterizem prática de *spam*.
- Caracterize prática de *flood*[12].
- De cunho comercial e/ou pertencentes a "correntes" ou "pirâmides" de qualquer espécie.

- Acessar indevidamente ou sem autorização às caixas postais de terceiros. As tentativas de acesso deverão ser registradas em *log*.
- Enviar informações críticas para pessoas ou organizações não autorizadas. Quando for o caso, devem ser observadas as orientações para o tratamento de informações classificadas.
- Enviar mensagens não solicitadas para múltiplos destinatários, exceto por intermédio da administração e se relacionadas a uso legítimo da instituição.
- Participar em Listas de Discussão que possam abordar assuntos alheios ao INCA, suas diretorias e suas gerências, exceto em casos de participação em Listas de Discussão sobre assuntos relacionados às atividades desenvolvidas no INCA.
- Efetuar compras não autorizadas pela *Internet*.
- Manipular identificadores para mascarar a origem de qualquer mensagem ou publicação transmitida através do serviço de *e-mail* institucional.
- Utilizar *Bots* ou outros métodos automatizados para acessar o serviço de *e-mail* institucional, adicionar ou baixar contatos, enviar ou redirecionar mensagens.

12 Flood é o ato de enviar uma grande quantidade (enxurrada ou inundação) de mensagens para uma mesma pessoa.

2.4.5.5 Sistema Corporativo de Informação

É vedado a todos os Usuários, dentre outros similares:

- Desenvolver, gerar, compilar, copiar, coletar, propagar, executar ou tentar introduzir qualquer código fonte de *software* projetado para se auto-replicar, danificar ou de outra maneira obstruir o acesso, afetar o desempenho ou tentar acessar indevidamente qualquer computador, da rede de computadores ou de um SISTEMA CORPORATIVO DE INFORMAÇÃO.

É vedado a todos os Usuários usar cada SISTEMA CORPORATIVO DE INFORMAÇÃO para:

- Fazer a engenharia reversa, descompilar, desmontar, decifrar ou, de outro modo, tentar copiar o código fonte de um SISTEMA CORPORATIVO DE INFORMAÇÃO ou de qualquer tecnologia relacionada, ou de qualquer parte deles.

2.4.5.6 Meios de Armazenamento de Dados

É vedado a todos os Usuários, dentre outros similares:

- Compartilhar pastas na ESTAÇÃO DE TRABALHO.
- Usar as áreas de armazenamento para a manutenção de arquivos de músicas e filmes protegidos por direitos autorais ou conteúdo ofensivo, exceto por necessidade do serviço e sob supervisão técnica da **GERÊNCIA DE RECURSOS TECNOLÓGICOS**.

2.4.5.7 Meios de Impressão

Em nenhuma hipótese o usuário deverá abrir o equipamento mediante a utilização de ferramentas.

3 DISPOSIÇÕES FINAIS

Devem ser observadas as penalidades dispostas na **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.

Deve observado disposto na **POLÍTICA DE RESPONSABILIDADES EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES**.

Devem ser observadas as competências e as responsabilidades do **COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** com relação aos DOCUMENTOS COMPLEMENTARES, conforme o disposto no **DOCUMENTO DE CONSTITUIÇÃO DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES**.

Os casos omissos e as dúvidas com relação a esta POLÍTICA devem ser submetidos ao **COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.