Concessão de Conta de Acesso Pessoal

DIRETRIZES E NORMAS

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

Dispõe sobre as orientações, as regras, as responsabilidades e as proibições mandatórias associadas à disciplina de solicitação, de concessão e de revogação de contas de acesso pessoal para usuários, destinadas a utilização dos recursos computacionais, disponibilizados e mantidos pelo INCA para uso corporativo.

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 **COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES,** 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 as orientações, as regras, as responsabilidades e as proibições mandatórias associadas à disciplina de solicitação, de concessão e de revogação de contas de acesso pessoal para usuários, destinada à utilização dos recursos computacionais, disponibilizados e mantidos pelo INCA.

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 encontra-se publicada e disponibilizada, pelo **SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO (STI)**, 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.

2 CONCESSÃO DE ACESSO PESSOAL

2.1 Acesso Biométrico

A CONTA DE ACESSO BIOMÉTRICO, quando implementada, deve ser vinculada a uma CONTA DE ACESSO e ambas devem ser utilizadas para se obter um acesso, a fim de atender os conceitos da autenticação de múltiplos fatores.

Os dados biométricos devem ser tratados como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

2.2 Contas de Acesso Pessoal

2.2.1 Diretrizes Gerais

Todos os USUÁRIOS INTERESSADOS (todo o PÚLICO-ALVO deste DOCUMENTO) têm direito a uma CONTA DE ACESSO, observadas as condições dispostas neste DOCUMENTO e na **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES**.

Será concedida uma CONTA DE ACESSO somente após a data de contratação ou de entrada em exercício do USUÁRIO INTERESSADO.

Cada USUÁRIO INTERESSADO, que não exerça funções de administração da rede local, poderá ser titular de uma única CONTA DE ACESSO individual, enquanto perdurar o seu vínculo com o INCA ou conforme previsto no item “Revogação da Conta de Acesso (Desativação)”, deste DOCUMENTO.

Somente USUÁRIOS cadastrados para execução de tarefas específicas na administração de ATIVOS DE INFORMAÇÃO poderão utilizar CONTA DE ACESSO no perfil de administrador.

Cada CONTA DE ACESSO é pessoal, intransferível e não podendo ser compartilhada com outras pessoas em nenhuma hipótese, devendo estar associada a uma pessoa física e atrelada inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

Todos os USUÁRIOS INTERESSADOS deverão, por meio do **TERMO DE RESPONSABILIDADE**, assumir o compromisso de:

- Declarar o conhecimento e aceitação dos termos deste DOCUMENTO e de suas normas complementares, não podendo a qualquer tempo alegar desconhecimento ou ignorância.
- Declarar estar ciente de que os acessos realizados à Internet, assim como conteúdo das mensagens de e-mail institucional são passíveis de auditoria.
- Manter a confidencialidade de sua SENHA DO USUÁRIO, alterando a mesma sempre que existir qualquer indício de possível comprometimento ou em intervalos regulares de tempo.

Quando a CONTA DE ACESSO for concedida (deferimento da solicitação do USUÁRIO INTERESSADO) o USUÁRIO CREDENCIADO passa a ser automaticamente o responsável, perante o INCA e a legislação (cível e criminal), pelo uso correto de sua CONTA DE ACESSO.

- O USUÁRIO CREDENCIADO será devidamente responsabilizado por eventuais quebras de segurança ocorrida com a utilização de sua respectiva CONTA DE ACESSO.
- Se existir CONTA DE ACESSO de uso compartilhado por mais de um USUÁRIO CREDENCIADO, a responsabilidade perante o INCA e a legislação (cível e criminal) será dos USUÁRIOS que dela se utilizarem. Se for identificado que o gestor tem conhecimento ou tenha solicitação o uso compartilhado, ele será responsabilizado.
- Falhas nas tentativas de acesso (login) devem ser auditadas pela ÁREA DE RECURSOS TECNOLÓGICOS.
- São as possíveis naturezas de cada CONTA DE ACESSO:
    - Conta de Acesso à rede interna, ao *e-mail* institucional e à Internet.

- Conta de Acesso a cada SISTEMA CORPORATIVO DE INFORMAÇÃO.

2.2.1.1 Contas de Acesso à Rede Interna, ao *e-mail Institucional* e à *Internet*

É de competência da **GERÊNCIA DE RECURSOS TECNOLÓGICOS**, hierarquicamente ligada a Divisão de Tecnologia da Informação (DTI), a administração e o controle dos acessos à REDE INTERNA DE COMUNICAÇÃO DE DADOS do INCA, ao *e-mail* institucional e à *Internet*.

As informações armazenadas na REDE INTERNA DE COMUNICAÇÃO DE DADOS do INCA e no *e-mail* institucional são de uso e acesso restritos.

Cada USUÁRIO CREDENCIADO poderá ser titular de uma única caixa postal individual no Servidor de Correio Eletrônico, com direitos de envio/recebimento de mensagens, enquanto perdurar o seu vínculo com o INCA.

O Usuário não poderá ter CONTA DE ACESSO com perfil de administrador, nem com privilégio de administrador local da ESTAÇÃO DE TRABALHO.

Depois de criada a CONTA DE ACESSO à REDE INTERNA DE COMUNICAÇÃO DE DADOS do INCA, o usuário poderá ter um espaço no SERVIDOR DE ARQUIVOS da REDE INTERNA DE COMUNICAÇÃO DE DADOS para guardar seus arquivos de trabalho.

- O acesso ao SERVIDOR DE ARQUIVOS da REDE INTERNA DE COMUNICAÇÃO DE DADOS será estruturado em perfis de acesso, definidos pela **GERÊNCIA DE RECURSOS TECNOLÓGICOS**, com base na atividade exercida e setor de lotação do solicitante.
- Arquivos gravados apenas localmente nos computadores (por exemplo, no drive C:) não terão garantia de *backup* e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio USUÁRIO CREDENCIADO.
- Arquivos pessoais (fotos, músicas, vídeos, etc..) não podem ser copiados ou movidos para o SERVIDOR DE ARQUIVOS, pois podem sobrecarregar o armazenamento nos servidores. Caso

identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem comunicação prévia ao usuário.

2.2.1.2 Contas de Acesso a cada Sistema Corporativo de Informação

É de competência da **GERÊNCIA DE DESENVOLVIMENTO DE SISTEMAS**, hierarquicamente ligada a Divisão de Tecnologia da Informação (DTI), a administração e o controle de acesso às informações armazenadas em cada SISTEMA CORPORATIVO DE INFORMAÇÃO e no seu respectivo Banco de Dados, que é de uso e acesso restrito.

O acesso a cada SISTEMA CORPORATIVO DE INFORMAÇÃO será estruturado em níveis de acesso, com base na atividade exercida e setor de lotação do solicitante.

O acesso deve ser controlado pelo próprio SISTEMA CORPORATIVO DE INFORMAÇÃO, através de um procedimento que estabeleça a identidade do usuário com algum grau de confiança (autenticação), e só então devem ser concedidos determinados privilégios (autorização) de acordo com esta identidade.

Cada SISTEMA CORPORATIVO DE INFORMAÇÃO deverá ter algum mecanismo que impeça a mesma CONTA DE ACESSO de estar ativa, simultaneamente, em mais de uma ESTAÇÃO DE TRABALHO.

Cada SISTEMA CORPORATIVO DE INFORMAÇÃO deverá ter algum mecanismo que impeça a exibição automática, na tela de *login*, da SENHA DO USUÁRIO referente ao respectivo *login* em uso.

Cada CONTA DE ACESSO só poderá ser reinicializada por ação do detentor, através mecanismo sistêmico pelo qual o próprio USUÁRIO CREDENCIADO informe a antiga SENHA DO USUÁRIO e, posteriormente, a nova SENHA DO USUÁRIO, ou ainda, por solicitação formal do USUÁRIO CREDENCIADO à **GERÊNCIA DE DESENVOLVIMENTO DE SISTEMAS**. Em casos de extrema necessidade de reinicializar uma SENHA DO USUÁRIO, isto só poderá ocorrer mediante a confirmação de algumas informações de caráter pessoal do USUÁRIO CREDENCIADO. Nestes casos, o operador deverá retornar a

ligação para confirmação desses dados. Para casos considerados críticos, a solicitação de reinicialização de conta deverá ser feita através de contato com o Gerente de TI.

Caso o USUÁRIO CREDENCIADO suspeite do comprometimento de sua SENHA DO USUÁRIO, esta deverá ser modificada imediatamente.

A gestão operacional de cada SISTEMA CORPORATIVO DE INFORMAÇÃO permanecerá em sua Unidade de origem, cabendo a **GERÊNCIA DE DESENVOLVIMENTO DE SISTEMAS**, apenas a administração do controle de acesso.

Todos os acessos serão providos via perfis de trabalho ou por uma solicitação especial feita ao PROPRIETÁRIO DA INFORMAÇÃO envolvida. A existência de acessos privilegiados, não significa por si só, que um indivíduo esteja autorizado a usar esses privilégios.

Os direitos e perfis de acesso seguem as definições do servidor público responsável pelo USUÁRIO INTERESSADO em concordância com os padrões estabelecidos pela área de TI.

Qualquer mudança funcional e de lotação ou atribuições dentro da organização implicará na revisão dos direitos de acesso do USUÁRIO CREDENCIADO.

Qualquer mudança no quadro funcional referente a desligamentos ou afastamentos de um USUÁRIO CREDENCIADO implicará em remoção imediata das autorizações concedidas. Todo ativo produzido pelo USUÁRIO CREDENCIADO desligado deverá ser mantido, garantindo o reconhecimento e o esclarecimento da propriedade do acervo para o INCA.

Será indeferida a Solicitação para Concessão de Conta de Acesso a Sistema Corporativo ou bloqueado o acesso já concedido a um USUÁRIO CREDENCIADO por solicitação da APADS (Assessoria de Procedimentos Administrativos Disciplinares e Sindicantes) responsável pelo recebimento da denúncia e do andamento do PAD (Processo Administrativo Disciplinar) ou por sentença condenatória pela prática de crime na forma dolosa.

O pedido indeferido poderá ser reiterado e o acesso bloqueado ser restabelecido após cumprimento da pena ou sanção, bem como, após a conclusão do processo que vier a absolver o processado, sempre mediante manifestação favorável da **GERÊNCIA DE DESENVOLVIMENTO DE SISTEMAS** e da **GERÊNCIA DE RECURSOS TECNOLÓGICOS**, baseada na conveniência administrativa e com fundamento nos princípios da administração pública.

2.2.2 Solicitação de Conta de Acesso

É de competência do servidor público (responsável pelo departamento ao qual o USUÁRIO INTERESSADO estiver vinculado) solicitar formalmente uma CONTA DE ACESSO para um USUÁRIO INTERESSADO, através de formulário específico (**SOLICITAÇÃO DE SERVIÇO CORPORATIVO DE TI**) assinado, estando a solicitação condicionada ao respectivo deferimento.

- Nos casos em que o usuário já possua a CONTA DE ACESSO, mas que ainda não tenha assinado tal formulário, a assinatura do mesmo deve ser obtida em caráter de urgência.

O USUÁRIO INTERESSADO deve preencher e assinar o **TERMO DE RESPONSABILIDADE**, no qual declara conhecer e se obriga a respeitar as recomendações, as políticas, os padrões, as normas e os procedimentos do INCA relacionados ao ambiente de TI (incluindo as instruções contidas neste DOCUMENTO), bem como as implicações legais decorrentes do não cumprimento do disposto no termo.

Nos casos em que o usuário já possua a CONTA DE ACESSO, mas que ainda não tenha assinado tal termo, a assinatura do mesmo deve ser obtida em caráter de urgência.

O USUÁRIO INTERESSADO deve preencher e assinar o **TERMO DE CONFIDENCIALIDADE**, no qual declara conhecer e se obriga a respeitar o sigilo dos dados, informações e conhecimentos do INCA.

- Nos casos em que o usuário já possua a CONTA DE ACESSO, mas que ainda não tenha assinado tal termo, a assinatura do mesmo deve ser obtida em caráter de urgência.

2.2.3 Análise da Solicitação de Conta de Acesso

É de competência da **GERÊNCIA DE RECURSOS TECNOLÓGICOS** ou da **GERÊNCIA DE DESENVOLVIMENTO DE SISTEMAS**, conforme a natureza da solicitação de CONTA DE ACESSO, efetuar a análise do documento de SOLICITAÇÃO DE CONTA DE ACESSO e deferir ou indeferir o pedido.

A análise da SOLICITAÇÃO DE CONTA DE ACESSO está condicionada a apresentação de todos os documentos relacionados no subitem anterior ("Solicitação de Conta de Acesso"), devidamente preenchidos e assinados.

A SOLICITAÇÃO DE CONTA DE ACESSO poderá ser indeferida sempre que for julgada improcedente (pela **GERÊNCIA DE DESENVOLVIMENTO DE SISTEMAS** ou pela **GERÊNCIA DE RECURSOS TECNOLÓGICOS**, conforme o caso).

2.2.4 Concessão de Conta de Acesso

As autorizações serão concedidas de acordo com:

- As necessidades de desempenho das funções e considerando o princípio do menor privilégio.
- Comprovação da autorização do PROPRIETÁRIO DA INFORMAÇÃO.

O USUÁRIO INTERESSADO somente terá o acesso solicitado após o deferimento de seu pedido, resultando na concessão de uma CONTA DE ACESSO.

A concessão de CONTA DE ACESSO a um USUÁRIO INTERESSADO que não faça parte do quadro funcional do INCA, deverá atender a necessidade e a conveniência da prestação do serviço público e dependerá de solicitação e autorização da chefia imediata (assinatura do servidor público), na qual o usuário estiver prestando os serviços, estando à autorização do credenciamento vinculada a **GERÊNCIA**

DE DESENVOLVIMENTO DE SISTEMAS ou pela **GERÊNCIA DE RECURSOS TECNOLÓGICOS**, conforme o caso.

Cada CONTA DE ACESSO é composta por uma IDENTIFICAÇÃO DO USUÁRIO e uma SENHA DO USUÁRIO vinculada a esta.

Identificação do Usuário (Identificação da Conta de Acesso)

A cada usuário deve ser disponibilizada apenas uma IDENTIFICAÇÃO DO USUÁRIO que deve ser única, pessoal e intransferível.

A IDENTIFICAÇÃO DO USUÁRIO é um identificador individualizado que assegura a responsabilidade de cada usuário por suas ações.

Senha do Usuário (Senha da Conta de Acesso)

A SENHA DO USUÁRIO é pessoal e intransferível, não devendo (independente das circunstâncias) ser fornecida, compartilhada ou divulgada com outras pessoas que não seja o usuário autorizado, ficando o proprietário da senha responsável legal por qualquer prática indevida cometida.

A SENHA DO USUÁRIO qualifica o usuário como responsável por todos os acessos realizados.

Recomenda-se que a SENHA DO USUÁRIO seja criptografada antes de ser armazenada na base de dados.

O usuário deve trocar sua SENHA DO USUÁRIO periodicamente, seguindo as orientações da área de TI.

A cada nova CONTA DE ACESSO que for criada, deve ser fornecida uma SENHA DO USUÁRIO inicial e temporária, devendo ser gerada de forma que já entre expirada no sistema, exigindo sua

alteração no próximo *login* do usuário. A SENHA DO USUÁRIO não deve ser enviada ao usuário através de terceiros ou de mensagens de *e-mail* desprotegidas (não criptografadas).

O fornecimento de SENHA DO USUÁRIO temporária, nos casos de esquecimento por parte do usuário, deve ser efetuado somente após a identificação positiva do respectivo usuário.

Em caso de suspeita ou comprovação de exposição indevida do ambiente de TI do INCA, todas as SENHAS DOS USUÁRIOS devem ser imediatamente alteradas.

2.2.4.1 Composição da Identificação do Usuário

A IDENTIFICAÇÃO DO USUÁRIO deve ser única e ter o formato da matrícula funcional.

Caso uma IDENTIFICAÇÃO DO USUÁRIO para um novo Usuário seja a mesma de outro já existente, fica facultado ao administrador do RECURSO COMPUTACIONAL utilizar outro formato para a IDENTIFICAÇÃO DO USUÁRIO.

2.2.4.2 Composição da Senha do Usuário

São recomendações para a composição da SENHA DO USUÁRIO:

- **Obrigatoriedade de Quantidade Mínima de Caracteres**: Recomenda-se adotar um padrão definido onde a senha tenha uma quantidade mínima de caracteres.
- **Utilização de Caracteres Alfabéticos**: Recomenda-se adotar um padrão definido onde a senha possa conter também caracteres alfabéticos.
- **Utilização de *Case Sensitive***: Recomenda-se adotar um padrão definido onde a senha possa conter também caracteres alfabéticos maiúsculos e minúsculos.
- **Utilização de Caracteres Numéricos**: Recomenda-se adotar um padrão definido onde a senha possa conter também caracteres numéricos.

- **Utilização de Caracteres Especiais**: Recomenda-se adotar um padrão definido onde a senha possa conter também caracteres especiais como: @ # $ % & *.
- **Inibição de Reutilização**: Recomenda-se adotar um padrão definido onde seja inibida a reutilização de senhas pelo mesmo usuário.
- **Inibição de Datas**: Recomenda-se adotar um padrão definido onde seja inibida a utilização de senhas que combinem formatos de datas do calendário. Exemplo: DDMMAAAA
- **Inibição de Números Comuns**: Recomenda-se adotar um padrão definido onde seja inibida a utilização de senhas que combinem formatos de placas (ou marcas de carros), números de telefone ou outros números comuns.
- **Inibição do Nome do Usuário**: Recomenda-se adotar um padrão definido onde seja inibida a utilização de senhas contendo o nome integral ou parcial do usuário. Exemplo: 1221jose. Exemplo: Jose Luiz 1221. Exemplo: Jose 2015.
- **Inibição da Matrícula ou Identificador do Usuário**: Recomenda-se adotar um padrão definido onde seja inibida a utilização de senhas contendo a matrícula ou identificador (ID) do usuário. Exemplo: m22028. Exemplo: m22028jose. Exemplo: Jose m22028.
- **Inibição do Nome do Sistema Operacional**: Recomenda-se adotar um padrão definido onde seja inibida a utilização de senhas contendo o nome do sistema operacional.
- **Inibição de Nomes Próprios**: Recomenda-se adotar um padrão definido onde seja inibida a utilização de senhas contendo nomes próprios. Exemplo: 1221jose.
- **Inibição de Sequências**: Recomenda-se adotar um padrão definido onde seja inibida a utilização de senhas contendo sequências Numéricas (Exemplo: 123jose), Alfabéticas (Exemplo: ABCjose, abcJose) ou de Caracteres Especiais.
- **Inibição de Caracteres Seguidos do Teclado do Computador**: Recomenda-se adotar um padrão definido onde seja inibida a utilização de senhas contendo caracteres seguidos do teclado do computador. Exemplo: ASDFG, YUIOP, asdfg, yuiop.

Recomenda-se adotar um padrão definido onde seja proibido que a senha contenha o nome da empresa ou uma abreviatura do mesmo.

2.2.5 Validade da Conta de Acesso

São recomendações para a validade da SENHA DO USUÁRIO:

- **Data de Expiração**: Recomenda-se adotar um padrão definido onde as SENHAS DOS USUÁRIOS possuem prazo de validade com 30 ou 45 dias, obrigando a renovação da mesma.
- **Troca Forçada**: Recomenda-se adotar um padrão definido onde o Usuário seja forçado a trocar a SENHA DO USUÁRIO no primeiro acesso (*login*).
- **Bloqueio Automático**: Recomenda-se adotar um padrão definido onde CONTA DE ACESSO seja bloqueada após a 3ª (tentativa) tentativa de acesso (*login*).

2.2.6 Responsabilidades do Usuário pela Conta de Acesso

O USUÁRIO CREDENCIADO é inteiramente responsável:

- Pelo uso de sua CONTA DE ACESSO à REDE INTERNA DE COMUNICAÇÃO DE DADOS, bem como, sua SENHA DO USUÁRIO e outros tipos de autorização. que são de uso individual e intransferível, não podendo assim ser compartilhados com terceiros. CONTAS DE ACESSO são individuais e não compartilhadas, salvo em situações especiais que a Unidade julgar necessárias, e dentro de prazos curtos e pré-determinados.
- Por ações indevidas que venham a ser efetuadas a partir de sua CONTA DE ACESSO, inclusive no caso alguém obter o acesso à sua conta, devido à não utilização de senhas seguras ou a descuido quanto a guarda da SENHA DO USUÁRIO.
- Pela manutenção da SENHA DO USUÁRIO de forma segura, devendo seguir normas e procedimentos padronizados pela Gerência de Tecnologia da Informação.

2.2.7 Monitoramento da Conta de Acesso

A **ÀREA DE RECURSOS TECNOLÓGICOS** reserva-se o direito de monitorar todas as Contas de Acesso, a qualquer tempo e sem aviso prévio, com o objetivo de verificar possíveis violações ou tentativas de violações a **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES**.

Todas as atividades dos USUÁRIOS CREDENCIADOS que afetem cada SISTEMA CORPORATIVO DE INFORMAÇÃO devem ser possíveis de reconstituição a partir dos *logs* de maneira a evitar ou dissuadir o comportamento incorreto. Estes procedimentos devem contar inclusive com mecanismos de responsabilização claros e amplamente divulgados nos meios de comunicação internos.

2.2.8 Revogação da Conta de Acesso (Desativação)

Uma CONTA DE ACESSO deverá ser revogada quando do desligamento do usuário.

Uma CONTA DE ACESSO poderá ser revogada, estando o pedido condicionado ao preenchimento de formulário específico (**SOLICITAÇÃO DE SERVIÇO CORPORATIVO DE TI**), contendo a IDENTIFICAÇÃO DO USUÁRIO, justificativa, autorização da chefia imediata (servidor público) e autorização do procedimento como um todo, exarado pela **GERÊNCIA DE RECURSOS TECNOLÓGICOS** (com relação ao primeiro formulário supracitado) ou pela **GERÊNCIA DE DESENVOLVIMENTO DE SISTEMAS** (com relação ao segundo formulário supracitado), conforme o caso.

O pedido deve ser enviado a **GERÊNCIA DE DESENVOLVIMENTO DE SISTEMAS** ou a **GERÊNCIA DE RECURSOS TECNOLÓGICOS**, conforme o caso.

Todos os formulários, referentes ao deferimento do pedido, devem ser obrigatoriamente arquivados digitalmente em um repositório comum e com acesso controlado.

São situações previstas inicialmente para a revogação da CONTA DE ACESSO de um USUÁRIO CREDENCIADO (não se limitando a estas):

- Por Afastamento Definitivo ou Desligamento

- É de competência da **GERÊNCIA DE RECURSOS HUMANOS** solicitar a revogação da CONTA DE ACESSO do respectivo usuário (quando se tratar de servidor público) ou do servidor público responsável pelo departamento ao qual o usuário estiver vinculado (quando se tratar de um prestador de serviços – "Terceirizado").
- É de competência do servidor público responsável (chefia imediata) pelo respectivo USUÁRIO CREDENCIADO revisar imediatamente seus arquivos armazenados em sua ESTAÇÃO DE TRABALHO ou em qualquer servidor de rede e, também, seus documentos em papel para determinar quem tornar-se-á curador das informações relacionadas, assim como nos casos devidos, identificar o método mais adequado para a eliminação das mesmas, levando-se em conta as orientações sobre a eliminação de informações classificadas contidas na legislação vigente.

- Por Violação ou Tentativa de Violação da POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
  - A **ÀREA DE RECURSOS TECNOLÓGICOS** reserva-se o direito de revogar (desativa), a qualquer tempo e sem aviso prévio, todas as CONTAS DE ACESSO que violarem ou tentarem violar a **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.
- Por Inatividade
  - A **ÀREA DE RECURSOS TECNOLÓGICOS** reserva-se o direito de desativar, a qualquer tempo e sem aviso prévio, todas as CONTAS DE ACESSO que estiverem Inativas:

2.2.9 Bloqueio da Conta de Acesso (Suspensão)

- Por Afastamento Temporário
  - . Em caso de afastamento temporário do usuário de suas funções de trabalho, o bloqueio de uma CONTA DE ACESSO poderá ser solicitado (conforme o caso) pela

GERÊNCIA DE RECURSOS HUMANOS ou pelo servidor público responsável pelo departamento ao qual o USUÁRIO CREDENCIADO estiver vinculado.

- Por Violação ou Tentativa de Violação da POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
  - A **ÀREA DE RECURSOS TECNOLÓGICOS** reserva-se o direito de bloquear (suspender), a qualquer tempo e sem aviso prévio, todas as CONTAS DE ACESSO que violarem ou tentarem violar a **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.
- Por Tentativas Frustradas de Acesso (*Login*)
  - Recomenda-se limitar o número de tentativas frustradas (incorretas) de acesso (*login*), bloqueando temporariamente a CONTA DE ACESSO e desfazendo a conexão.
  - Esse procedimento protege o usuário titular da CONTA DE ACESSO, pois diminui os riscos de alguém tentar adivinhar as senhas, informando repetidamente Senhas incorretas. Atingido esse limite, só o administrador do sistema poderá desbloquear a CONTA DE ACESSO, por exemplo.

2.2.10 Arquivamento da Solicitação de Conta de Acesso

Todos os formulários, referentes ao deferimento ou ao indeferimento do pedido, devem ser obrigatoriamente arquivados digitalmente.

2.2.11 Sistemas de Controle de Senhas

Deve ser configurado para proteger as SENHAS DOS USUÁRIOS armazenadas contra uso não autorizado, sem apresentá-las na tela do computador, mantendo-as em arquivos criptografados e estipulando datas de expiração (normalmente se recomenda a troca de senhas após 30 ou 45 dias).

Para evitar o uso frequente das mesmas SENHAS DOS USUÁRIOS, o sistema de controle de senhas deve manter um histórico das últimas senhas utilizadas por cada USUÁRIO CREDENCIADO.

2.3 Proibições aos Usuários

São diretrizes específicas proibitivas que devem ser observadas e respeitadas por cada Usuário quanto a cometer ou ser cúmplice de atos considerados impróprios à conduta profissional adequada:

Com relação aos RECURSOS COMPUTACIONAIS, é vedado a todos os Usuários, dentre outros similares:

- Adotar condutas que interfiram na operação normal e adequada dos RECURSOS COMPUTACIONAIS 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*. Essas configurações são padronizadas, conforme definições da área de TI. Havendo a necessidade de alteração destas configurações, a solicitação deve ser encaminhada à área de TI 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 (*malwares*) 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 RECURSOS COMPUTACIONAIS 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 usar os RECURSOS COMPUTACIONAIS, 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 RECURSOS COMPUTACIONAIS, 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.

É vedado a todos os Usuários, dentre outros similares:

- Obter ou tentar obter indevidamente a SENHA DO USUÁRIO de qualquer outro Usuário Credenciado, chave criptográfica ou qualquer outro mecanismo de Controle de Acesso que possa possibilitar o acesso não autorizado aos RECURSOS COMPUTACIONAIS do INCA, tais como, tentativas de fraudar a autenticação de um Usuário ou a segurança de qualquer servidor de rede. Cabe ressaltar que, o uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).
- Fornecer, compartilhar ou divulgar (independente das circunstâncias) a sua SENHA DO USUÁRIO.

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 ESTRATÉGICO E GESTOR DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.