DIÁRIO OFICIAL DA UNIÃO

Publicado em: 17/12/2025 | Edição: 240 | Seção: 1 | Página: 44

Órgão: Ministério do Desenvolvimento Agrário e Agricultura Familiar/Instituto Nacional de Colonização e Reforma Agrária

PORTARIA Nº 1.510, DE 16 DE DEZEMBRO DE 2025

Estabelece a Política de Gestão do Controle de Acesso no âmbito do Instituto Nacional de Colonização e Reforma Agrária - Incra.

O PRESIDENTE DO INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA - INCRA, no uso das atribuições que lhe são conferidas pelo Decreto n.º 11.232, de 10 de outubro de 2022, alterado pelo Decreto n.º 12.171, de 09 de setembro de 2024, combinado com o art. 143 do Regimento Interno da Autarquia, aprovado pela Portaria n.º 925, de 30 de dezembro de 2024, publicada no Diário Oficial da União do dia 31 de dezembro de 2024; resolve:

Art. 1º Fica instituída, no âmbito do Instituto Nacional de Colonização e Reforma Agrária - Incra, a Política de Gestão do Controle de Acesso, em complemento às diretrizes estabelecidas pelo art. 12, da Política de Segurança da Informação - PoSIC (ref. Processo Administrativo nº 54000.018337/2022-16).

CAPÍTULO I

DO ESCOPO

Art. 2º A Política de Gestão do Controle de Acesso tem como objetivo estabelecer diretrizes, competências e responsabilidades para sistematizar controles de identificação, autenticação e autorização para salvaguardar as informações do Incra, estejam elas em qualquer meio, seja físico ou digital, a fim de evitar a quebra de segurança da informação e quaisquer acessos não autorizados que implique em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Art. 3º Esta política abrange diretrizes, competências e responsabilidades sobre como o acesso às informações e recursos são concedidos, monitorados e revogados dentro do Incra de forma a garantir que apenas pessoas autorizadas tenham acesso às informações e recursos necessários para desempenhar suas funções, minimizando assim o risco de violações de segurança e vazamento de dados. Ela inclui diversos elementos, como por exemplo:

I - identificação e autenticação de usuários;

II - determina quais recursos, sistemas ou informações os usuários tem permissão para acessar após a autenticação bem sucedida (definição de privilégios e níveis de acesso de acordo com as responsabilidades de cada usuário);

III - gerencia o acesso a sistemas, dados digitais, acesso físico a edifícios, salas de servidor e outros locais que abrigam informações críticas;

IV - estabelece práticas para monitorar e registrar as atividades de acesso para identificar potenciais ameaças ou violações de segurança;

V - define diretrizes para revogar o acesso de um usuário, como por exemplo demissão, mudança de função ou quando o acesso se torna desnecessário para suas responsabilidades;

VI - envolve a conscientização de usuários sobre a importância do controle de acesso, as melhores práticas de segurança e a importância de proteger as credenciais de acesso.

VII - todas as informações, cuja o Incra seja o agente de tratamento, ao meio utilizado para este tratamento, seja digital ou físico, e as dependências físicas desta organização, bem como a qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento. Especificamente, inclui os funcionários que trabalham para o Incra, sejam servidores efetivos ou temporários, os contratados e terceiros, parceiros que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação do Incra.

Art. 4˚ O Incra deve definir regras de limitação ou restrição de acesso aos colaboradores, para que estes disponham de privilégios mínimos necessários para exercerem suas atividades, funções e responsabilidades pré-definidas.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 5º Para fins de compreensão dos termos utilizados nesta política serão utilizados os seguintes conceitos e definições:

I.acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

ameaça: conjunto de fatores externos com o potencial de causar dano para um sistema ou organização;

ativo: tudo que tenha valor para a organização, material ou não;

ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

backup/cópia de segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

banco de dados: coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;

comitê de segurança da informação e comunicação (CSIC): grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal;

computação em nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem;

conta de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

conta de serviço: conta de acesso à rede corporativa de computadores, necessária a um procedimento automático (aplicação, script, entre outros) sem qualquer intervenção humana no seu uso;

controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estrutura organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

controles de segurança: certificado que autoriza uma pessoa natural para o tratamento de informação classificada;

CTIR GOV - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, Segurança Institucional da Presidência da República;

documento: unidade de registro de informações, qualquer que seja o suporte ou o formato;

e-mail: sigla de correio eletrônico (electronic mail); XXI - eliminação: exclusão de dado ou conjunto de dados, armazenados em banco de dados, independentemente do procedimento empregado;

equipe de tratamento e resposta a incidentes cibernéticos (ETIR): grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade;

evento: qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Em outras palavras, qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao cliente;

evento de segurança: qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança;

firewall: ferramenta para evitar acesso não autorizado, tanto na origem quanto no destino, a uma ou mais redes. Podem ser implementados por meio de hardware ou software, ou por meio de ambos. Cada mensagem que entra ou sai da rede passa pelo firewall, que a examina a fim de determinar se atende ou não os critérios de segurança especificados;

incidente: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

incidente cibernético: ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema;

incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

internet: rede global, composta pela interligação de inúmeras redes;

medidas de segurança: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;

MFA: sigla de autenticação de multifatores (multifactor authentication);

política: intenções e diretrizes globais formalmente expressas pela direção;

prestador de serviço: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso;

rede de computadores: conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação;

recursos de processamento da informação: qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem;

risco: no sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

risco de segurança da informação: risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

segurança da informação: preservação da confidencialidade, integridade, disponibilidade, adicionalmente outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas;

serviços: meio de fornecimento de valor a clientes, com vistas a entregar os resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos;

SI: sigla de segurança da informação;

sistema de informação: conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada;

tecnologia da informação: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas, utilizados para obter, processar, armazenar, disseminar e fazer uso de informações; e

usuário: pessoa física ou jurídica, seja servidor público, estudante ou prestador de serviços, voluntário habilitado pela administração para acessar os ativos de informação do Incra.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 6º Esta política considera os seguintes princípios:

I - respeito aos princípios e diretrizes constitucionais, legais e regulamentares que regem a Administração Pública Federal;

II - garantia de integridade, autenticidade e disponibilidade da informação sob a custódia do Incra, com respeito ao princípio da transparência e atribuição de confidencialidade apenas nos casos expressamente previstos na legislação;

III - alinhamento estratégico da Política de Segurança da Informação - PoSIC com os demais planos institucionais;

IV - responsabilidade pelo cumprimento das normas pertinentes à segurança da informação vigentes; e

V - conscientização, educação e comunicação como alicerces fundamentais para o fomento da cultura em segurança da informação.

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 7º As diretrizes gerais constituem os pilares do controle de acesso no Incra, orientando a elaboração de norma, processo, planos, procedimentos, metodologia e ações de controle que garantem que os princípios básicos de segurança da informação sejam alcançados.

§ 1º Procedimento operacional padrão deve ser estabelecido, documentado e atualizado para implementar controles de acesso físicos e lógicos à informação e aos ativos associados à informação que são por ele gerenciados ou custodiados, com objetivo de proteger adequadamente a confidencialidade das informações não públicas, bem como a integridade e a disponibilidade das informações consideradas críticas para o negócio.

§ 2º Os controles de acesso devem ser implementados para identificação, autenticação e autorização garantindo que apenas usuários autorizados tenham acesso físico ou lógico aos recursos, sistemas ou serviços de TI.

§ 3º Rotinas devem ser configuradas para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuário, administrador e serviço para ativos e software institucionais devem ser estabelecidas e mantidas atualizadas.

§ 4º Sempre que possível controles de acesso devem ser implementados conforme necessidade legítima que justifique o acesso à informação por pessoa, sistema ou entidade, seguindo o princípio "privilégio mínimo", o qual estabelece que o perfil de acesso concedido deve incluir apenas os poderes necessários para atender as legítimas necessidades.

§ 5º Quando possível, os controles de acesso lógicos no Incra devem utilizar autenticação com certificado digital, a fim de proporcionar uma identificação inequívoca de pessoas físicas e jurídicas, assim como comprovação de autoria em transações digitais.

§ 6º Os direitos de acesso lógicos e físicos devem ser analisados criticamente, a intervalos regulares, para remover direitos que deixaram de ser necessários e para assegurar que privilégios indevidos não foram obtidos.

§ 7º Os controles de autorização, identificação e autenticação devem garantir que apenas usuários autorizados tenham acesso físico ou façam uso dos sistemas de informação do Incra.

CAPÍTULO V

ACESSO LÓGICO

Art. 8º O acesso lógico aos recursos da Rede Local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela Coordenação-Geral de Tecnologia e Gestão da Informação, baseado nas responsabilidades e tarefas de cada usuário, logo:

I - o Incra deve implementar protocolos de comunicação e redes seguros.

II - terão direito a acesso lógico aos recursos da Rede Local os usuários de recursos de tecnologia da informação.

III - para fins desta Portaria, consideram-se usuários de recursos de tecnologia da informação servidores ocupantes de cargo efetivo, temporário ou cargo em comissão, ocupantes de emprego público em exercício, assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade no Incra, que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação do Incra.

IV - o acesso remoto deve ser realizado por meio de VPN - Rede Virtual Privada, após as devidas autorizações.

V - deve ser utilizado o MFA para a autenticação de acesso remoto.

VI - o acesso a todas as aplicações corporativas ou de terceiros que estejam hospedados em fornecedores deve utilizar MFA.

VII - o Incra deve centralizar a autenticação, autorização e auditoria (AAA) dos ativos de informação da sua infraestrutura de rede.

VIII - o Incra deve adotar técnicas de segmentação de rede visando limitar o acesso de forma eficiente e segura, assegurando que apenas colaboradores e dispositivos autorizados possam interagir com partes específicas da rede.

Art. 9º O Incra deve estabelecer e manter um inventário de todas as contas gerenciadas, este deve incluir contas de usuário, administrativas, testes e serviço. Em caso de contas de serviço, o inventário deve conter no mínimo informações de:

I - área de negócio proprietária.

II - data de criação/última autorização de renovação de acesso;

III - a Coordenação-Geral de Tecnologia e Gestão da Informação é responsável por validar todas as contas ativas do órgão a cada 90 dias;

Art. 10. A Coordenação-Geral de Tecnologia e Gestão da Informação deve implementar a centralização da gestão de contas por meio de serviço de diretório e/ou identidade.

Art. 11. A Coordenação-Geral de Tecnologia e Gestão da Informação deve estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, tal inventário deve ser revisado periodicamente.

Art. 12. A Coordenação-Geral de Tecnologia e Gestão da Informação deve centralizar o controle de acesso para todos os ativos de informação da organização por meio de um serviço de diretório ou provedor de SSO.

Art. 13. A Coordenação-Geral de Tecnologia e Gestão da Informação deve definir e manter o controle de acesso dos usuários baseado em funções, logo:

I - deve ser elaborada a documentação dos direitos dos acessos para cada função dentro da organização.

II - a Coordenação-Geral de Tecnologia e Gestão da Informação deverá realizar análises de controle de acesso aos ativos institucionais para validar se todos os privilégios estão autorizados para a execução de atividades de cada função, este processo deve ser repetido de forma periódica ou quando novas funções e ativos de informação forem inseridos na organização.

III - ao conceder acesso a usuários que lidam com dados pessoais, deve-se limitar, estritamente, o acesso aos sistemas que processam esses dados ao mínimo necessário para cumprir os objetivos essenciais do processamento, em conformidade com o princípio da minimização de dados. Ao atribuir ou revogar os direitos de acesso concedidos deve-se incluir:

a) verificação de que o nível de acesso concedido é apropriado às políticas de acesso, além de ser consistente com outros requisitos, tais como, segregação de funções;

b) garantia de que os direitos de acesso não estão ativados antes que o procedimento de autorização esteja completo;

c) manutenção de um registro preciso e atualizado dos perfis dos usuários criados para os que tenham sido autorizados a acessar o sistema de informação e os dados pessoais neles contidos;

d) mudança dos direitos de acesso dos usuários que tenham mudado de função ou de atividades, e imediata remoção ou bloqueio dos direitos de acesso dos usuários que deixaram o Incra;

e) analisar criticamente os direitos de acesso em intervalos regulares;

f) analisar e aprovar, ad referendum, os pedidos de acesso a dados institucionais, por meio de APIs (Apllication Programming Interface) disponibilizadas no Conecta Gov.br, e ratificar os novos acessos no Comitê de Governança Digital - CGD e comunicar ao Comitê de Segurança da Informação e Comunicação - CSIC;

g) disponibilizar, em ferramenta própria, funcionalidade para que as unidades organizacionais, proprietárias de dados, possam avaliar e aprovar pedidos de acesso a seus respectivos dados, antes de atribuir direitos de acessos.

Art. 14. A Coordenação-Geral de Tecnologia e Gestão da Informação deve implementar um processo formal de registro de usuários que tratem de dados pessoais para permitir atribuição de direitos de acesso e fornecer medidas para lidar com o comprometimento do controle de acesso do usuário, como corrupção ou comprometimento de senhas ou outros dados de registro do usuário, para tanto podem ser realizadas as seguintes ações:

I - o uso de um identificador de usuário único, para permitir relacionar os usuários com suas responsabilidades e ações;

II - o uso compartilhado de identificador de usuário somente será permitido, onde eles são necessários por razões operacionais ou de negócios e deverá ser aprovado e documentado;

III - a garantia de que o um mesmo identificador de usuário não é emitido para outros.

CAPÍTULO VI

CONTA DE ACESSO LÓGICO E SENHA

Art. 15. Para utilização das estações de trabalho do Incra, será obrigatório o uso de uma única identificação (login) e de senha de acesso, fornecidos pela Coordenação-Geral de Tecnologia e Gestão da Informação, mediante solicitação formal pelo titular da unidade do requisitante, sendo assim, fazem-se necessários:

I - o preenchimento do formulário de solicitação de acesso se encontra disponível no Sistema Eletrônico de Informações - SEI;

II - a definição, pela unidade requisitante ao qual o usuário está vinculado, os privilégios de acesso dos usuários à Rede Local, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

III - na necessidade de utilização de perfil diferente do disponibilizado, o titular da unidade do usuário deverá encaminhar solicitação para a Coordenação-Geral de Tecnologia e Gestão da Informação, que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Art. 16. O login e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pela Coordenação-Geral de Tecnologia e Gestão da Informação quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo titular da unidade do requisitante.

Art. 17. O padrão adotado para o formato da conta de acesso do usuário é a sequência primeiro nome + ponto + último nome do usuário, como por exemplo, joao.silva.

Parágrafo único. Nos casos de já existência de conta de acesso para outro usuário, a Coordenação-Geral de Tecnologia e Gestão da Informação realizará outra combinação utilizando o nome completo do usuário para o qual a conta está sendo criada.

Art. 18. O padrão adotado para o formato da senha é o definido pela Coordenação-Geral de Tecnologia e Gestão da Informação, que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores, sendo assim:

I - a formação da senha da identificação (login) de acesso à Rede Local deve seguir as regras de:

a) possuir tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras e números, para contas que utilizam MFA e 14 (catorze) caracteres para contas que não utilizam MFA;

b) recomenda-se a utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &,...);

c) não ser formada por sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações;

d) não utilizar termos óbvios, tais como: Brasil, senha, usuário, password ou system;

e) não reutilizar as últimas 05 (cinco) senhas.

II - a Coordenação-Geral de Tecnologia e Gestão da Informação fornecerá uma senha temporária para cada conta de acesso criada no momento da liberação dessa conta e a mesma deverá ser alterada pelo usuário quando do primeiro acesso à Rede Local.

Art. 19. As senhas de acesso serão renovadas a cada 90 dias, devendo o usuário ser informado antecipadamente, a fim de que ele próprio efetue a mudança.

Parágrafo único. Caso não efetue a troca no prazo estabelecido, será bloqueado seu acesso à Rede Local até que a nova senha seja configurada.

CAPÍTULO VII

BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

Art. 20. A conta de acesso será bloqueada nos seguintes casos:

I - após 5 tentativas consecutivas de acesso errado;

II - solicitação do superior imediato do usuário com a devida justificativa;

III - quando da suspeita de mau uso dos serviços disponibilizados pelo Incra ou descumprimento da Política de Segurança da Informação - PoSIC e normas correlatas em vigência;

IV - após 90 dias consecutivos sem movimentação pelo usuário.

Art. 21. O desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do superior imediato do usuário à Coordenação-Geral de Tecnologia e Gestão da Informação.

Art. 22. Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato ou da unidade de Recursos Humanos.

Art. 23. A conta de acesso não utilizada há mais de 180 dias poderá ser cancelada.

Art. 24. O Incra deve garantir a implementação de um processo formal de cancelamento de usuários que administrem ou operem sistemas e serviços que tratem de dados pessoais. Tal processo deverá incluir:

I - a imediata remoção ou desabilitação de usuário que tenha deixado o Incra;

II - a remoção e identificação, de forma periódica, ou a desabilitação de usuários com os mesmos identificadores.

Art. 25. A Coordenação-Geral de Tecnologia e Gestão da Informação deve configurar o bloqueio automático de sessão nos ativos após um período de inatividade preestabelecido. Tal prazo pode ser específico para cada tipo de ativo.

Art. 26. A Coordenação-Geral de Tecnologia e Gestão da Informação deve, sempre que possível, priorizar a revogação/desativação de contas com o objetivo de manter dados e logs para possíveis auditorias.

CAPÍTULO VIII

ACESSO FÍSICO

Art. 27. O Incra deve definir perímetros de segurança para proteger ambientes e ativos contra acesso físico não autorizado, danos e interferências de acordo com as diretrizes a seguir:

I - definir a localização e resistência dos perímetros de acordo com os requisitos de segurança da informação relacionados aos ativos que se encontre dentro dos perímetros;

II - proteger os ambientes seguros contra acessos não autorizados por meio de mecanismos de controle de acesso, como fechaduras tradicionais ou digitais, que possibilitem autenticação por biometria, senhas, PINs ou cartões de acesso. Sendo assim:

a) o Incra deve executar testes nos mecanismos de controle de acesso em períodos pré-definidos para assegurar a funcionalidade total do equipamento;

b) os mecanismos de controle de acesso devem ser monitorados pela Coordenação-Geral de Tecnologia e Gestão da Informação.

III - estabelecer uma área de recepção ou outros meios de controle de acesso físico a ambientes que não for conveniente a implementação de mecanismos de controle de acesso.

Art. 28. O acesso físico a ambientes seguros ou ativos de tratamento e armazenamento de dados do Incra é destinado apenas a pessoal autorizado.

Art. 29. O Incra deve manter um processo de gestão de acessos para fornecimento, revisão periódica, atualização e revogação das autorizações.

Art. 30. O Incra deve implementar e manter seguro logs ou registro físico de todos os acessos aos ativos de informação.

Art. 31. O acesso a ambientes seguros ou ativos de tratamento e armazenamento de dados por fornecedores ou prestadores de serviços será concedido somente quando necessário e de acordo com as seguintes diretrizes:

I - para fins específicos e autorizados;

II - autorização concedida pela Coordenação-Geral de Tecnologia e Gestão da Informação;

III - supervisionado e monitorado.

Art. 32. Os ativos de armazenamento e tratamento de dados que se encontrem fora do Incra devem ser protegidos contra perda, roubos, danos e acesso físico não autorizados conforme as seguintes diretrizes:

I - não deixar o ativo sem vigilância em locais públicos e inseguros;

II - proteger o ativo contra riscos associados a visualização de informações por outra pessoa;

III - implementar as funcionalidades de rastreamento e limpeza remota.

Art. 33. O Incra deve estabelecer uma política ou normativo equivalente sobre a gestão de mídias de armazenamento, de acordo com as seguintes diretrizes:

I - exigir autorização para a saída de mídias de armazenamento do Incra;

II - armazenar mídias em local seguro de acordo com a classificação de suas informações;

III - criptografar as mídias de acordo com a classificação de suas informações;

IV - manter cópias de segurança de mídias de acordo com a classificação de suas informações.

Art. 34. O Incra deve elaborar política, ou normativo equivalente, que defina condições e restrições pertinentes ao acesso físico nos dispositivos de trabalho remoto, levando em consideração as seguintes diretrizes:

I - segurança física do local de trabalho remoto;

II - regras e orientações quanto ao acesso de familiares e visitantes ao dispositivo.

CAPÍTULO IX

MOVIMENTAÇÃO INTERNA

Art. 35. Quando houver mudança do usuário para outra unidade ou o usuário ocupar uma nova função, os direitos de acesso à Rede Local devem ser revogados, sendo que:

I - o novo superior imediato deve realizar a solicitação de novos acessos de acordo com nova unidade/função do usuário;

II - os direitos de acesso antigos devem ser imediatamente cancelados, conforme solicitação do antigo superior imediato.

CAPÍTULO X

CONTA DE ACESSO BIOMÉTRICO

Art. 36. A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para se obter um acesso, a fim de atender os conceitos da autenticação de multifatores (MFA).

Parágrafo único. O Incra deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO XI

ADMINISTRADORES

Art. 37. A utilização de identificação (login) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação. Sendo que:

I - somente os técnicos da Coordenação-Geral de Tecnologia e Gestão da Informação, devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede;

II - na necessidade de utilização de login com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para a Coordenação-Geral de Tecnologia e Gestão da Informação, que poderá negar os casos em que entender desnecessária a utilização;

III - se concedida a permissão ao usuário como administrador local na estação de trabalho, esse será responsável por manter a integridade da máquina, não podendo instalar, desinstalar ou remover qualquer programa sem autorização formal da Coordenação-Geral de Tecnologia e Gestão da Informação;

IV - caso constatada a irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão;

V - a identificação (login) com privilégio de administrador nos equipamentos locais será fornecida em caráter provisório, podendo ser renovada por solicitação formal do titular da unidade requisitante;

VI - salvo para atividades específicas da área responsável pela gestão da tecnologia da informação do órgão, não será concedida, para um mesmo usuário, identificação (login) com privilégio de administrador para mais de uma estação de trabalho, ou para acesso a equipamentos servidores e a dispositivos de rede;

VII - excepcionalmente, poderão ser concedidas identificações (login) de acesso à rede de comunicação de dados a visitante em caráter temporário após apreciação do superior imediato, por meio do Recursos Humanos;

VIII - a Coordenação-Geral de Tecnologia e Gestão da Informação deve implementar o MFA para todas as contas de administrador;

IX - a Coordenação-Geral de Tecnologia e Gestão da Informação deve restringir os privilégios de administrador a contas de administrador dedicados nos ativos de informação, para que o usuário com privilégio de administrador não consiga realizar atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, estas atividades deverão ser realizadas preferencialmente a partir da conta primária não privilegiada do usuário;

X - ao tratar dados pessoais a Coordenação-Geral de Tecnologia e Gestão da Informação observar o princípio do privilégio mínimo como regra, para garantir que o usuário receba apenas os direitos mínimos necessários para executar suas atividades, para tanto podem ser realizadas as seguintes ações:

a) remover os direitos de administrador nos dispositivos finais;

b) remover todos os direitos de acesso root e admin aos servidores e utilizar tecnologias que permitam a elevação granular de privilégios conforme a necessidade, ao mesmo tempo em que fornecem recursos claros de auditoria e monitoramento;

c) eliminar privilégios permanentes (privilégios que estão "sempre ativos") sempre que possível;

d) limitar a associação de uma conta privilegiada ao menor número possível de pessoas;

e) minimizar o número de direitos para cada conta privilegiada.

CAPÍTULO XII

RESPONSABILIDADES

Art. 38. É de responsabilidade do superior imediato do usuário comunicar formalmente aos Recursos Humano e à Coordenação-Geral de Tecnologia e Gestão da Informação o desligamento ou saída do usuário do Incra, para que as permissões de acesso à Rede Local sejam canceladas.

Art. 39. Caberá aos Recursos Humanos do Incra a criação, desbloqueio e revogação de permissões de acesso aos recursos via automação.

Art. 40. É responsabilidade dos Recursos Humanos do Incra a comunicação imediata à Coordenação-Geral de Tecnologia e Gestão da Informação sobre desligamentos, férias e licenças de funcionários de empresas prestadoras de serviços, para que seja efetuado o bloqueio momentâneo ou revogação definitiva da permissão de acesso aos recursos. Ademais:

I - os serviços serão filtrados por programas de antivírus, anti-phishing e anti-spam e, caso violem alguma regra de configuração, serão bloqueados ou excluídos automaticamente;

II - nenhum usuário do Incra terá acesso ao conteúdo das informações armazenadas nos equipamentos servidores do Instituto sem autorização da unidade competente.

Art. 41. É de responsabilidade da Coordenação-Geral de Tecnologia e Gestão da Informação o monitoramento da utilização de serviços de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como bloquear, temporariamente, sem aviso prévio, a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica do Incra.

Art. 42. O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à Rede Local e a recursos de tecnologia custodiados ou de propriedade do Incra, logo:

I - o usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos;

II - a utilização simultânea da conta de acesso à Rede Local em mais de uma estação de trabalho ou notebook deve ser evitada, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica;

III - o usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à Rede Local.

Art. 43. O usuário deve informar à Coordenação-Geral de Tecnologia e Gestão da Informação qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 44. É dever de o usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a Instituição, a saber:

I - não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;

II - evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;

III - interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;

IV - não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;

V - não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

VI - utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;

VII - não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis;

VIII - assinar o Termo de Responsabilidade (Modelo - Anexo I) quanto a utilização da respectiva conta de acesso.

CAPÍTULO XIII

DISPOSIÇÕES GERAIS

Art. 45. Os incidentes que afetem a segurança das informações, assim como o descumprimento da Política de Segurança da Informação - PoSIC e Normas de Segurança, devem ser obrigatoriamente comunicados pelos usuários à Coordenação-Geral de Tecnologia e Gestão da Informação.

Art. 46. Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a Coordenação-Geral de Tecnologia e Gestão da Informação fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização, e considerando que:

I - nos casos em que o ator da quebra de segurança for um usuário, a Coordenação-Geral de Tecnologia e Gestão da Informação comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis;

II - ações que violem a PoSIC, ou que quebrem os controles de Segurança da Informação, serão passíveis de sansões civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente;

III - processo administrativo disciplinar específico deverá ser instaurado para apurar as ações que constituem em quebra das diretrizes impostas por esta Norma e pela PoSIC;

IV - a resolução de casos de violação/transgressões omissos nas legislações correlatas será resolvida pelo Comitê de Segurança da Informação - CSI do Incra.

Art. 47. Esta Portaria entra em vigor na data de sua publicação.

CÉSAR FERNANDO SCHIAVON ALDRIGHI

ANEXO

Modelo de Termo de Responsabilidade

SERVIÇO PÚBLICO FEDERAL

Instituto Nacional de Colonização e Reforma Agrária - Incra

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, e lotado no(a)_____deste Ministério, DECLARO , sob pena das sanções cabíveis nos termos da _____ (legislação vigente) que assumo a responsabilidade por:

I - tratar o(s) ativo(s) de informação como patrimônio do Instituto Nacional de Colonização e Reforma Agrária - Incra;

II - utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do Incra;

III - contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 27 de maio de 2020, que Dispõe sobre Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal;

IV - utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do Incra;

V - responder, perante o Incra pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

VI - acessar a rede corporativa, computadores, Internet e/ou utilização de e-mail, somente com autorização (usuário/senha), por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail;

VII - utilizar o correio eletrônico (e-mail) colocado a minha disposição somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail;

VIII - não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

IX - manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

X - não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador (browser), bloquear estação de trabalho, bem como encerrar a seção do cliente de correio, garantindo assim a impossibilidade de acesso indevido por terceiros;

XI - não revelar minha senha de acesso à rede corporativa, computadores, Internet e/ou do correio eletrônico (e-mail) a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

XII - responder em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

<<Local>>, <<UF>>, <<dia>> de <<mês >> de <<ano>>.

Assinaturas
Nome do usuário Unidade organizacional
Nome da autoridade responsável pela autorização do acesso Unidade organizacional

	10. Celebrar, pelo menos, 5 (cinco) atos internacionais, voltados para a cooperação na área de defesa com Nações Amigas. (CAE/SCAI)
	11. Atender a, pelo menos, 10 (dez) solicitações de visitas oficiais de delegações estrangeiras, ligadas à área de defesa, ao Brasil. (CAE/SCAI)
	12. Cumprir, pelo menos, 90% das atividades relacionadas à participação em eventos desenvolvidos por Organismos Internacionais. (CAE/SCOI)
	13. Acompanhar e, se for o caso, identificar oportunidades de participação do Brasil em missões de paz da ONU. (CAE/SCOI)
	14. Participar, presencial ou por videoconferência, de eventos desenvolvidos por Organismos Internacionais de Interesse do Ministério da Defesa. (CAE/SCOI)
	15. Cumprir pelo menos uma atividade prevista para a CPLP e/ou PROSUL (presencial ou videoconferência). (CAE/SCOI)
	16. Participar de pelo menos uma atividade prevista para a JID e/ou CMDA. (CAE/SCOI)
	17. Realizar, no mínimo, uma atividade de interesse da Defesa relacionada com o desarmamento (presencial ou videoconferência). (CAE/SCOI)
	18. Participar de, no mínimo, de uma reunião de trabalho/seminário/videoconferência envolvendo os assuntos relacionados com a ZOPACAS, BRICS, CPLP, IBAS, OTCA, MERCOSUL, e/ou Consenso de Brasília. (CAE/SCOI)
	19. Atingir anualmente 100% das visitas técnicas para renovação de inscrição (programadas) e inscrição (inopinadas), bem como o controle de Originais de Aerolevantamento. (CHELOG/SUBLOP)
	20. Realizar anualmente 80% das atividades de contribuição para a preservação das características e para a interação entre os sistemas de ensino das Forças Armadas, da Escola Superior de Guerra (ESG) e da Escola Superior de Defesa (ESD) e os órgãos de interesse. (CHEC)
	21. Realizar anualmente cursos, atividades acadêmicas, concursos, cooperações e debates de temas ligados à Defesa Nacional no âmbito da sociedade brasileira. (CHEC)
	22. Executar anualmente 80% das atividades planejadas de promoção à realização de pesquisas científicas em temas de interesse da Defesa Nacional no âmbito da sociedade brasileira. (CHEC)
	23. Executar anualmente 80% dos recursos orçamentários anuais destinados aos projetos de preservação do Patrimônio Histórico e Cultural Militar. (CHEC)

Ministério do Desenvolvimento Agrário e Agricultura Familiar

INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA

PORTARIA Nº 1.499, DE 15 DE DEZEMBRO DE 2025

Reconhece famílias de Comunidades Quilombolas, localizados no estado do Pará, para acesso às políticas públicas do Programa Nacional de Reforma Agrária - PNRA.

O PRESIDENTE DO INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA - INCRA, no uso das atribuições que lhe são conferidas pelo Decreto n.º 11.232, de 10 de outubro de 2022, alterado pelo Decreto n.º 12.171, de 09 de setembro de 2024, combinado com o art. 143 do Regimento Interno da Autarquia, aprovado pela Portaria n.º 925, de 30 de dezembro de 2024, publicada no Diário Oficial da União do dia 31 de dezembro de 2024; e

Considerando que a reforma agrária visa promover a melhor distribuição de terra mediante modificações no regime de posse e uso, a fim de atender aos princípios de justiça social, desenvolvimento rural sustentável, aumento de produção e promoção social, conforme preconiza o Programa Nacional de Reforma Agrária - PNRA;

Considerando o Parecer n. 00011/201/CGA/PFE-INCRA-SEDE/PGF/AGU (25786868), que conclui pela possibilidade de inclusão das comunidades quilombolas como beneficiárias do Programa Nacional de Reforma Agrária para fins de acesso a políticas públicas respectivas;

Considerando o disposto contido na Portaria/INCRA/P/nº 175, de 19 de abril de 2016, publicada no Diário Oficial da União n.º 75, de 20 de abril de 2016, (25786906), para reconhecimento de indivíduos ou famílias quilombolas para fins de acesso às políticas do PNRA;

Considerando o Decreto n.º 9.311, de 15 de março de 2018, que dispõe sobre o processo de seleção, permanência e titulação das famílias beneficiárias do Programa Nacional de Reforma Agrária e seu artigo 11;

Considerando o Parágrafo único do artigo 2º do Decreto n.º 11.995, de 15 de abril de 2024, que institui o programa "Terra da Gente" que se destina a atender o público beneficiário da Política Nacional de Reforma Agrária;

Considerando o constante dos autos do processo administrativo n.º 54000.167863/2025-51, resolve:

Art. 1º Reconhecer os 44 (quarenta e quatro) territórios quilombolas localizados no estado do Pará, reconhecido pelo Instituto de Terras do Pará - ITERPA, descritos no anexo abaixo;

Art. 2º Autorizar o processo de análise para a inclusão de 3247 (três mil e duzentos e quarenta e sete) famílias, para acesso às políticas públicas do Programa Nacional de Reforma Agrária - PNRA pela Plataforma de Governança Territorial - PGT de unidades familiares cadastradas no Cadastro Único para Programas Sociais do Governo Federal (CadÚnico), conforme o Decreto n.º 11.016, de 2022, nos termos do art. 7º do Decreto n.º 9.311, de 2018.

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

CÉSAR FERNANDO SCHIAVON ALDRIGHI

ANEXO

Lista das comunidades quilombolas

SR	COMUNIDADE	MUNICÍPIO	ÁREA (HA)	Famílias	SIPRA
PA - 01	RAMAL DO BACURI	ABAETETUBA	911,8576	72	PA1129000
PA - 01	QUILOMBO SÃO JORGE	ABAETETUBA	61,7185	12	PA1091000
PA - 01	ARIENGA - ESTRADA	ABAETETUBA E BARCARENA	50,9494	23	PA1092000
PA - 01	VILA CRUZEIRO	ABAETETUBA E BARCARENA	622,5738	19	PA1093000
PA - 01	ALTO ACARÁ - AMARQUALTA	ACARÁ	12409,4000	398	PA0728000
PA - 01	JABAQUARA	ACARÁ	56,1960	57	PA1094000
PA - 01	MENINO JESUS	ACARÁ	634,0861	35	PA1095000
PA - 01	COMUNIDADE DO ESPIRITO SANTO	ACARÁ	276,1594	30	PA1096000
PA - 01	TATITUQUARA, SÃO SEBASTIÃO, AJARÁ E BOA ESPERANÇA	BAGRE	7662,7691	41	PA0744000
PA - 01	QUILOMBOS DE BALIEIRO	BAGRE	2998,2990	28	PA1097000
PA - 01	QUILOMBO VILA DUTRA	BAIÃO	213,1133	83	PA1098000
PA - 01	SÃO JOSÉ DO ICATU	BAIÃO E MOCAJUBA	3034,2753	170	PA1099000
PA - 01	QUILOMBOS CUXIU	BONITO e SÃO MIGUEL DO GUAMÁ e OURÉM	353,0204	85	PA1130000
PA - 01	AMÉRICA	BRAGANÇA	106,9587	100	PA1101000
PA - 01	QUILOMBOLA DE MOCAJUBA	BUJARU	510,3471	40	PA1102000
PA - 01	BOA ESPERANÇA	CAMETÁ	503,7489	42	PA0722000
PA - 01	QUILOMBOS - MAZAGÃO	CAMETÁ E MOCAJUBA	895,5784	50	PA1103000
PA - 01	SÃO PEDRO	CASTANHAL	362,5090	52	PA1104000
PA - 01	QUILOMBO NAVEGANTES	CASTANHAL	61,5415	20	PA1105000
PA - 01	MENINO JESUS DE PETIMANDEUA / PETIMANDEUA	INHANGAPI	302,0730	49	PA1106000
PA - 01	PARAISO	INHANGAPI	135,4017	22	PA1107000
PA - 01	REGIÃO DO RIO CAPIM / QUIANDEUA	IPIXUNA DO PARÁ	8118,7137	85	PA1108000
PA - 01	QUILOMBO DE IGARAPÉ - AÇU	MOCAJUBA	3332,9268	167	PA1109000
PA - 01	QUILOMBO DE AÇAIZAL	MOCAJUBA E MOJU	972,5264	55	PA1110000
PA - 01	JUQUIRI	MOJU	698,2962	65	PA1111000
PA - 01	QUILOMBO DE GUADALUPE	MOJU	448,6934	39	PA1112000
PA - 01	BAIXO GUAJARAÚNA, CACOAL, DIVINO ESPÍRTO SANTO, FAZENDA E CINCO REIS	MOJU E ABAETETUBA	1368,3736	46	PA1113000
PA - 01	IGARAPÉ DO ARIRÁ	OEIRAS DO PARÁ	1869,7987	56	PA1114000
PA - 01	QUILOMBOS DE BOM JESUS	OEIRAS DO PARÁ	113,9106	49	PA1115000
PA - 01	QUILOMBO AMÉRICA / NOVA AMÉRICA	OEIRAS DO PARÁ	7655,2272	331	PA1116000
PA - 01	QUILOMBO RIO BRANCO	OEIRAS DO PARÁ	256,6991	11	PA1117000
PA - 01	MONTEVIDÉU	OURÉM	49,4126	29	PA1118000
PA - 01	ATURIÁ	OURÉM	428,3112	165	PA1119000
PA - 01	ENGENHO NOVO	OURÉM	385,2366	56	PA1120000
PA - 01	QUILOMBO CEARAZINHO	OURÉM	10,5207	53	PA1121000
PA - 01	QUILOMBO SACATANDEUA	QUATIPURU	332,9457	24	PA1122000
PA - 01	VILA SANTÍSSIMA TRINDADE	SANTA IZABEL DO PARÁ	24,9472	115	PA1123000
PA - 01	QUILOMBO TRÊS VOLTAS	SANTA IZABEL DO PARÁ	1184,2208	18	PA1124000
PA - 01	QUILOMBOS DE CRAUATEUA / NOSSA SENHORA DE FÁTIMA DO CRAUATEUA	SÃO MIGUEL DO GUAMÁ	495,4909	42	PA1125000
PA - 01	ESPÍRITO SANTO DO ITÁ	STA. IZABEL DO PARÁ	16,6881	78	PA1126000
PA - 01	NOVA BETEL	TOMÉ AÇU	3039,0350	83	PA1127000
PA - 01	QUILOMBO PONTINHA	TRACUATEUA	115,1588	155	PA1128000
SM - 30	PEAFU	MONTE ALEGRE	1525,9261	49	SM0310000
SM - 30	QUILOMBOS UNIÃO SÃO JOÃO	PRAINHA	1806,8912	48	SM0330000

PORTARIA Nº 1.500, DE 15 DE DEZEMBRO DE 2025

Retifica a área do Projeto de Assentamento Queimada da Onça, código SIPRA PE0374000, localizado no município de Arcoverde, estado de Pernambuco.

O PRESIDENTE DO INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA - INCRA, no uso das atribuições que lhe são conferidas pelo Decreto n.º 11.232, de 10 de outubro de 2022, alterado pelo Decreto n.º 12.171, de 09 de setembro de 2024, combinado com o art. 143 do Regimento Interno da Autarquia, aprovado pela Portaria n.º 925, de 30 de dezembro de 2024, publicada no Diário Oficial da União do dia 31 de dezembro de 2024; e

Considerando os órgãos da Superintendência Regional de Pernambuco - SR(03)PE e da Diretoria de Obtenção de Terras - DT, que procederam à análise do processo administrativo n.º 54140.005131/2007-92 e decidiram pela regularidade da retificação de informações na Portaria/INCRA/SR-03/E/Nº 41, de 27 de dezembro de 2007, publicada no Diário Oficial da União do dia 07 de janeiro de 2008, que criou o Projeto de Assentamento Queimada da Onça, código SIPRA PE0374000, localizado no município de Arcoverde, estado de Pernambuco;

Considerando as informações do Projeto de Assentamento Queimada da Onça, a base cartográfica da SR(03)PE e a Nota Técnica n.º 5145/2025/SR(PE)D-1/SR(PE)/INCRA (SEI n.º 26518294), resolve:

Art. 1º Retificar a área de 715,5957 ha (setecentos e quinze hectares, cinquenta e nove ares e cinquenta e sete centiares), constante na Portaria/INCRA/SR-03/E/Nº 41, de 27 de dezembro de 2007, publicada no Diário Oficial da União do dia 07 de janeiro de 2008, que criou o Projeto de Assentamento Queimada da Onça, código SIPRA PE0374000, localizado no município de Arcoverde, estado de Pernambuco, para a área de 770,5941 ha (setecentos e setenta hectares, cinquenta e nove ares e quarenta e um centiares), em conformidade com a base cartográfica da SR(03)PE.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

CÉSAR FERNANDO SCHIAVON ALDRIGHI

PORTARIA Nº 1.501, DE 15 DE DEZEMBRO DE 2025

Retifica a capacidade de famílias do Projeto de Assentamento Ceres, código SIPRA RS0046000, localizado no município de Jóia, estado do Rio Grande do Sul.

O PRESIDENTE DO INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA - INCRA, no uso das atribuições que lhe são conferidas pelo Decreto n.º 11.232, de 10 de outubro de 2022, alterado pelo Decreto n.º 12.171, de 09 de setembro de 2024, combinado com o art. 143 do Regimento Interno da Autarquia, aprovado pela Portaria n.º 925, de 30 de dezembro de 2024, publicada no Diário Oficial da União do dia 31 de dezembro de 2024; e

Considerando os órgãos da Superintendência Regional do Rio Grande do Sul - SR(11)RS e da Diretoria de Obtenção de Terras - DT, que procederam à análise do processo administrativo n.º 21520.018896/1996-91 e apontaram uma irregularidade na retificação de informações na Portaria/INCRA/SR(11)RS/Nº 1135, de 23 de maio de 2025, publicada no Diário Oficial da União n.º 97, de 26 de maio de 2025, a qual retificou e tornou sem efeito a Portaria/INCRA/SR(11)RS/Nº 50, de 10 de dezembro de 1996, publicada no Diário Oficial da União n.º 240, de 11 de dezembro de 1996, que criou o Projeto de Assentamento Ceres, código SIPRA RS0046000, localizado no município de Jóia, no estado do Rio Grande do Sul;

Considerando as informações do Projeto de Assentamento, a base cartográfica da SR(11)RS, a Nota Técnica n.º 4456/2025/SR(11)RS-F4/SR(11)RS-F/SR(11)RS/INCRA (SEI n.º 26081055) e o Despacho (SEI n.º 26483042), resolve:

Art. 1º Convalidar a Portaria/INCRA/SR(11)RS/Nº 50, de 10 de dezembro de 1996, publicada no Diário Oficial da União n.º 240, de 11 de dezembro de 1996, que criou o Projeto de Assentamento Ceres, código SIPRA RS0046000, localizado no município de Jóia, no estado do Rio Grande do Sul.

Art. 2º Retificar a capacidade de 123 (cento e vinte e três) famílias, constante na Portaria/INCRA/SR(11)RS/Nº 1135, de 23 de maio de 2025, publicada no Diário Oficial da União n.º 97, de 26 de maio de 2025, para 119 (cento e dezenove) famílias, em conformidade com a base cartográfica da SR(11)RS.

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

CÉSAR FERNANDO SCHIAVON ALDRIGHI

PORTARIA Nº 1.502, DE 15 DE DEZEMBRO DE 2025

Reconhece indivíduos ou famílias do Território Quilombola do Carmo, código SIPRA SP0401000, situada no município de São Roque, estado do São Paulo, para fins de acesso às políticas do Programa Nacional de Reforma Agrária - PNRA.

O PRESIDENTE DO INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA - INCRA, no uso das atribuições que lhe são conferidas pelo Decreto n.º 11.232, de 10 de outubro de 2022, alterado pelo Decreto n.º 12.171, de 09 de setembro de 2024, combinado com o art. 143 do Regimento Interno da Autarquia, aprovado pela Portaria n.º 925, de 30 de dezembro de 2024, publicada no Diário Oficial da União do dia 31 de dezembro de 2024; e

Considerando que a reforma agrária visa promover a melhor distribuição de terra mediante modificações no regime de posse e uso, a fim de atender aos princípios de justiça social, desenvolvimento rural sustentável, aumento de produção e promoção social, conforme preconiza o Programa Nacional de Reforma Agrária - PNRA;

Considerando o Parecer n.º 00011/201/CGA/PFE-INCRA-SEDE/PGF/AGU (26263084), que conclui pela possibilidade de inclusão das comunidades quilombolas como beneficiárias do Programa Nacional de Reforma Agrária para fins de acesso a políticas públicas respectivas;

Considerando o disposto contido na Portaria/INCRA/P/Nº 175, de 19 de abril de 2016, publicada no Diário Oficial da União nº 75 de 20 de abril de 2016, (26263119), para reconhecimento de indivíduos ou famílias quilombolas para fins de acesso às políticas do PNRA;

Considerando o Decreto n.º 9.311, de 15 de março de 2018, que dispõe sobre o processo de seleção, permanência e titulação das famílias beneficiárias do Programa Nacional de Reforma Agrária e seu artigo 11;

Considerando o parágrafo único do art. 2º do Decreto n.º 11.995, de 15 de abril de 2024, que institui o programa "Terra da Gente" que se destina a atender o público beneficiário da Política Nacional de Reforma Agrária; e

Considerando o constante dos autos do processo administrativo n.º 54190.002991/2006-06, resolve:

Art. 1º Reconhecer 51 (cinquenta e uma) famílias do Território Quilombola do Carmo, código SIPRA SP0401000, com área de 347,5119 ha (trezentos e quarenta e sete hectares, cinquenta e um ares e dezenove centiares), localizado no município de São Roque, no estado de São Paulo.

Art. 2º Autorizar o processo de seleção pela Plataforma de Governança Territorial (PGT) de unidades familiares cadastradas no Cadastro Único para Programas Sociais do Governo Federal (CadÚnico), conforme o Decreto n.º 11.016, de 2022, como beneficiárias do PNRA, nos termos do art. 7º do Decreto n.º 9.311, de 15 de março de 2018.

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

CÉSAR FERNANDO SCHIAVON ALDRIGHI

PORTARIA Nº 1.503, DE 15 DE DEZEMBRO DE 2025

Retifica o número de famílias beneficiárias do Projeto de Assentamento Barra Nova, Código SIPRA MS0135000, localizado no município de Sidrolândia, no estado de Mato Grosso do Sul.

O PRESIDENTE DO INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA - INCRA, no uso das atribuições que lhe são conferidas pelo Decreto n.º 11.232, de 10 de outubro de 2022, alterado pelo Decreto n.º 12.171, de 09 de setembro de 2024, combinado com o art. 143 do Regimento Interno da Autarquia, aprovado pela Portaria n.º 925, de 30 de dezembro de 2024, publicada no Diário Oficial da União do dia 31 de dezembro de 2024; e

Considerando as manifestações da Superintendência Regional em Mato Grosso do Sul - SR(16)MS e da Diretoria de Obtenção de Terras - DT, que procederam à análise do Processo Administrativo n.º 54290.002673/2005-28, concluindo pela necessidade de retificação das informações constantes da Portaria/INCRA/SR-16/MS/Nº 41, de 27 de dezembro de 2005, publicada no Diário Oficial da União, de 29 de dezembro de 2005, que criou o Projeto de Assentamento Barra Nova, código SIPRA MS0135000, localizado no município de Sidrolândia, no estado de Mato Grosso do Sul;

Considerando as informações constantes do Projeto de Assentamento, a base cartográfica atualizada, os registros junto ao Cartório de Registro de Imóveis competente, bem como o disposto no Parecer n.º 27.600/2025/SR(16)MS-F4/SR(16)MS-F/SR(16)MS/INCRA, de 07 de novembro de 2025, resolve:

Art. 1º Retificar o número de famílias beneficiárias constante da Portaria/INCRA/SR-16/MS/Nº 41, de 27 de dezembro de 2005, publicada no Diário Oficial da União, de 29 de dezembro de 2005, que criou o Projeto de Assentamento Barra Nova, código SIPRA MS0135000, localizado no município de Sidrolândia, no estado de Mato Grosso do Sul, alterando o quantitativo de 320 (trezentas e vinte) unidades agrícolas para 269 (duzentas e sessenta e nove) unidades familiares, conforme informações dominiais e cadastrais atualizadas constantes do processo administrativo n.º 54290.002673/2005-28.

Art. 2º Permanecem inalteradas as demais disposições da Portaria/INCRA/SR-16/MS/Nº 41, de 27 de dezembro de 2005.

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

CÉSAR FERNANDO SCHIAVON ALDRIGHI

PORTARIA Nº 1.504, DE 15 DE DEZEMBRO DE 2025

Retificar área do Projeto de Assentamento Café Abelha, código SIPRA GO0062000, localizado no município de Doverlândia, no estado de Goiás.

O PRESIDENTE DO INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA - INCRA, no uso das atribuições que lhes são conferidas pelo Decreto n.º 11.232, de 10 de outubro de 2022, alterado pelo Decreto n.º 12.171, de 09 de setembro de 2024, combinado com o art. 143 do Regimento Interno da Autarquia, aprovado pela Portaria n.º 925, de 30 de dezembro de 2024, publicada no Diário Oficial da União do dia 31 de dezembro de 2024; e

Considerando que os órgãos da Superintendência Regional de Goiás - SR(04)GO e da Diretoria de Obtenção de Terras - DT, que procederam à análise do processo administrativo n.º 21450.001528/1996-20, e decidiram pela regularidade da retificação de informações na Portaria/INCRA/SR(04)GO/Nº 67, de 12 de dezembro de 1996, publicada no Diário Oficial da União n.º 242, Seção 1, Página 26.934, de 13 de dezembro de 1996, retificada no Diário Oficial da União n.º 202, Seção 1, Página 46, de 22 de outubro de 2001, que criou o Projeto de Assentamento Café Abelha, código SIPRA GO0062000, localizado no município de Doverlândia, no estado de Goiás;

Considerando a conformidade das informações do Projeto de Assentamento, a base cartográfica da SR(04)GO e a Nota Técnica n.º 3861/2025/SR(04)GO-T/SR(04)GO/INCRA (25668117), resolve:

Art. 1º Retificar a área de 1.141,8770 ha (um mil, cento e quarenta e um hectares, oitenta e sete ares e setenta centiares), constante da Portaria/INCRA/SR(04)GO/Nº 67, de 12 de dezembro de 1996, publicada no Diário Oficial da União nº 242, Seção 1, Página 26.934, de 13 de dezembro de 1996, retificada no Diário Oficial da União nº 202, Seção 1, Página 46, de 22 de outubro de 2001, que criou o Projeto de Assentamento Café Abelha, código SIPRA GO0062000, localizado no município de Doverlândia, no estado de Goiás, para a área de 1.141,3951 ha (um mil, cento e quarenta e um hectares, trinta e nove ares e cinquenta e um centiares).

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

CÉSAR FERNANDO SCHIAVON ALDRIGHI

PORTARIA Nº 1.505, DE 15 DE DEZEMBRO DE 2025

Retifica área e a capacidade do Projeto de Assentamento Santo Antônio II, código SIPRA PE0360000, localizado no município de Altinho, no estado de Pernambuco.

O PRESIDENTE DO INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA - INCRA, no uso das atribuições que lhe são conferidas pelo Decreto nº 11.232, de 10 de outubro de 2022, alterado pelo Decreto nº 12.171, de 09 de setembro de 2024, combinado com o art. 143 do Regimento Interno da Autarquia, aprovado pela Portaria nº 925, de 30 de dezembro de 2024, publicada no Diário Oficial da União do dia 31 de dezembro de 2024; e

Considerando os órgãos da Superintendência Regional de Pernambuco - SR(03)PE e da Diretoria de Obtenção de Terras - DT, que procederam à análise do processo administrativo n.º 54140.001622/2006-83 e decidiram pela regularidade da retificação de informações na Portaria/INCRA/SR-03/PE Nº 31, de 10 de agosto de 2006, publicada no Diário Oficial da União nº 159, Seção 1, de 18 de agosto de 2006, que criou o Projeto de Assentamento Santo Antônio II, código SIPRA PE0360000, localizado no município de Altinho, no estado de Pernambuco;

Considerando as informações do Projeto de Assentamento, a base cartográfica da SR(03)PE e a Nota Técnica n.º 5214/2025/SR(03)PE-D1/SR(03)PE/INCRA (26554113), resolve:

Art. 1º Retificar a área de 200,4871 ha (duzentos hectares, quarenta e oito ares e setenta e um centiares), constante na Portaria/INCRA/SR(03)PE/Nº 31, de 10 de agosto de 2006, publicada no Diário Oficial da União, nº 159, Seção 1, de 18 de agosto de 2006, que criou o Projeto de Assentamento Santo Antônio II, código SIPRA PE0360000, localizado no município de Altinho, no estado de Pernambuco, para a área de 195,8439 ha (cento e noventa e cinco hectares, oitenta e quatro ares e trinta e nove centiares).

Art. 2º Retificar a capacidade de assentamento de 17 (dezessete) unidades agrícolas familiares, constante na Retificação da Portaria/INCRA/SR(03)PE/Nº 31, de 10 de agosto de 2006, publicada no Diário Oficial da União, nº 228, Seção 1, de 29 de novembro de 2006, que criou o Projeto de Assentamento Santo Antônio II, código SIPRA PE0360000, localizado no município de Altinho, no estado de Pernambuco, para 15 (quinze) unidades agrícolas familiares.

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

CÉSAR FERNANDO SCHIAVON ALDRIGHI

PORTARIA Nº 1.507, DE 16 DE DEZEMBRO DE 2025

Retifica denominação do Projeto de Assentamento Estadual denominado Che Guevara, localizado no município de Mirante do Paranapanema, estado de São Paulo, sob gestão da Fundação Instituto de Terras do Estado de São Paulo José Gomes da Silva - ITESP.

O PRESIDENTE DO INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA - INCRA, no uso das atribuições que lhe são conferidas pelo Decreto n.º 11.232, de 10 de outubro de 2022, alterado pelo Decreto n.º 12.171, de 09 de setembro de 2024, combinado com o art. 143 do Regimento Interno da Autarquia, aprovado pela Portaria n.º 925, de 30 de dezembro de 2024, publicada no Diário Oficial da União do dia 31 de dezembro de 2024; e

Considerando os órgãos da Superintendência Regional de São Paulo - SR(08)SP e da Diretoria de Obtenção de Terras - DT, que procederam à análise do processo administrativo n.º 54190.000828/1998-84 e decidiram pela regularidade da convalidação das informações contidas na Portaria/INCRA/SR(08/Nº 17, de 08 de abril de 1998, publicada no Diário Oficial da União n.º 68, de 09 de abril de 1998, que criou o Projeto de Assentamento Estadual Che Guevara, código SIPRA SP0065000, localizado no município de Mirante do Paranapanema, no estado de São Paulo;

Considerando as informações do Projeto de Assentamento Estadual nos termos do Ofício n° 006/2025-ITESP-GSE-DPD (26390915) e Portaria ITESP 25/2024 (26390935), resolve:

Art. 1º Retificar a Portaria/INCRA/SR(08/Nº 17, de 08 de abril de 1998, publicada no Diário Oficial da União n.º 68, de 09 de abril de 1998, que criou o Projeto de Assentamento Estadual Che Guevara, código SIPRA SP0065000, localizado no município de Mirante do Paranapanema, no estado de São Paulo, alterando a denominação para Projeto de Assentamento Estadual - PE Irmã Dulce.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

CÉSAR FERNANDO SCHIAVON ALDRIGHI

PORTARIA Nº 1.509, DE 16 DE DEZEMBRO DE 2025

Reconhece e declara como terras da Comunidade Remanescente de Quilombo Alto Bonito, localizada no município de Brejo, no estado do Maranhão.

O PRESIDENTE DO INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA - INCRA, no uso das atribuições que lhe são conferidas pelo Decreto n.º 11.232, de 10 de outubro de 2022, alterado pelo Decerto n.º 12.171, de 09 de setembro de 2024, combinado com o art. 143 do Regimento Interno da Autarquia, aprovado pela Portaria n.º 925, de 30 de dezembro de 2024, publicada no Diário Oficial da União no dia 31 de dezembro de 2024; e

Considerando o disposto no art. 68 do Ato das Disposições Constitucionais Transitórias, nos arts. 215 e 216 da Constituição Federal de 1988, no Decreto n.º 4.887, de 20 de novembro de 2003, na Convenção Internacional n.º 169 da Organização Internacional do Trabalho (OIT), e nas normativas internas do Incra, bem como os termos do Relatório Técnico de Identificação e Delimitação (RTID), relativo à regularização das terras da Comunidade Quilombola Alto Bonito, publicado no Diário Oficial da União nos dias 18 e 21 de dezembro de 2015, retificado em 14 de julho de 2017, e no DOE/MA, nos dias 22 e 23 de dezembro de 2015, retificado em 14 de agosto de 2018; e, ainda, o que consta dos autos do Processo Administrativo n.º 54230.005031/2007-57, resolve:

Art. 1º Reconhecer e declarar como terras da Comunidade Remanescente de Quilombo Alto Bonito, a área de 3.806,3554 ha (Três mil oitocentos e seis hectares, trinta e cinco ares e cinquenta e quatro centiares), localizada no município de Brejo, no estado do Maranhão.

§1º Os limites e confrontações do território quilombola Penteado são: Norte: José Maria Bastos, José Oliveira de Aragão e Projeto de Assentamento Federal Árvores Verdes; Leste: Projeto de Assentamento Federal Árvores Verdes e Rio Parnaíba; Sul: Projeto de Assentamento Federal Santa Alice, Fazenda Depósito e Associação Comunitária dos Agricultores Remanescentes de Quilombo Data Arraial do Povoado Boa Vista; Oeste: imóvel Data Saco das Almas (área quilombola Saco das Almas).

§ 2º A planta e o memorial descritivo encontram-se disponíveis no processo administrativo n.º 54230.005031/2007-57 e no acervo fundiário do Incra pelo endereço eletrônico http://acervofundiario.incra.gov.br.

Art. 2º Esta Portaria entra em vigor sete dias após a data de sua publicação.

CÉSAR FERNANDO SCHIAVON ALDRIGHI

PORTARIA Nº 1.510, DE 16 DE DEZEMBRO DE 2025

Estabelece a Política de Gestão do Controle de Acesso no âmbito do Instituto Nacional de Colonização e Reforma Agrária - Incra.

O PRESIDENTE DO INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA - INCRA, no uso das atribuições que lhe são conferidas pelo Decreto n.º 11.232, de 10 de outubro de 2022, alterado pelo Decreto n.º 12.171, de 09 de setembro de 2024, combinado com o art. 143 do Regimento Interno da Autarquia, aprovado pela Portaria n.º 925, de 30 de dezembro de 2024, publicada no Diário Oficial da União do dia 31 de dezembro de 2024; resolve:

Art. 1º Fica instituída, no âmbito do Instituto Nacional de Colonização e Reforma Agrária - Incra, a Política de Gestão do Controle de Acesso, em complemento às diretrizes estabelecidas pelo art. 12, da Política de Segurança da Informação - PoSIC (ref. Processo Administrativo nº 54000.018337/2022-16).

CAPÍTULO I

DO ESCOPO

Art. 2º A Política de Gestão do Controle de Acesso tem como objetivo estabelecer diretrizes, competências e responsabilidades para sistematizar controles de identificação, autenticação e autorização para salvaguardar as informações do Incra, estejam elas em qualquer meio, seja físico ou digital, a fim de evitar a quebra de segurança da informação e quaisquer acessos não autorizados que implique em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Art. 3º Esta política abrange diretrizes, competências e responsabilidades sobre como o acesso às informações e recursos são concedidos, monitorados e revogados dentro do Incra de forma a garantir que apenas pessoas autorizadas tenham acesso às informações e recursos necessários para desempenhar suas funções, minimizando assim o risco de violações de segurança e vazamento de dados. Ela inclui diversos elementos, como por exemplo:

I - identificação e autenticação de usuários;

II - determina quais recursos, sistemas ou informações os usuários tem permissão para acessar após a autenticação bem sucedida (definição de privilégios e níveis de acesso de acordo com as responsabilidades de cada usuário);

III - gerencia o acesso a sistemas, dados digitais, acesso físico a edifícios, salas de servidor e outros locais que abrigam informações críticas;

IV - estabelece práticas para monitorar e registrar as atividades de acesso para identificar potenciais ameaças ou violações de segurança;

V - define diretrizes para revogar o acesso de um usuário, como por exemplo demissão, mudança de função ou quando o acesso se torna desnecessário para suas responsabilidades;

VI - envolve a conscientização de usuários sobre a importância do controle de acesso, as melhores práticas de segurança e a importância de proteger as credenciais de acesso.

VII - todas as informações, cuja o Incra seja o agente de tratamento, ao meio utilizado para este tratamento, seja digital ou físico, e as dependências físicas desta organização, bem como a qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento. Especificamente, inclui os funcionários que trabalham para o Incra, sejam servidores efetivos ou temporários, os contratados e terceiros, parceiros que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação do Incra.

Art. 4° O Incra deve definir regras de limitação ou restrição de acesso aos colaboradores, para que estes disponham de privilégios mínimos necessários para exercerem suas atividades, funções e responsabilidades pré-definidas.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 5º Para fins de compreensão dos termos utilizados nesta política serão utilizados os seguintes conceitos e definições:

I.acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

ameaça: conjunto de fatores externos com o potencial de causar dano para um sistema ou organização;

ativo: tudo que tenha valor para a organização, material ou não;

ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

backup/cópia de segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

banco de dados: coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;

comitê de segurança da informação e comunicação (CSIC): grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal;

computação em nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem;

conta de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

conta de serviço: conta de acesso à rede corporativa de computadores, necessária a um procedimento automático (aplicação, script, entre outros) sem qualquer intervenção humana no seu uso;

controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estrutura organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

controles de segurança: certificado que autoriza uma pessoa natural para o tratamento de informação classificada;

CTIR GOV - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, Segurança Institucional da Presidência da República;

documento: unidade de registro de informações, qualquer que seja o suporte ou o formato;

e-mail: sigla de correio eletrônico (electronic mail); XXI - eliminação: exclusão de dado ou conjunto de dados, armazenados em banco de dados, independentemente do procedimento empregado;

equipe de tratamento e resposta a incidentes cibernéticos (ETIR): grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade;

evento: qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Em outras palavras, qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao cliente;

evento de segurança: qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança;

firewall: ferramenta para evitar acesso não autorizado, tanto na origem quanto no destino, a uma ou mais redes. Podem ser implementados por meio de hardware ou software, ou por meio de ambos. Cada mensagem que entra ou sai da rede passa pelo firewall, que a examina a fim de determinar se atende ou não os critérios de segurança especificados;

incidente: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

incidente cibernético: ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema;

incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

internet: rede global, composta pela interligação de inúmeras redes;

medidas de segurança: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;

MFA: sigla de autenticação de multifatores (multifactor authentication);

política: intenções e diretrizes globais formalmente expressas pela direção;

prestador de serviço: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso;

rede de computadores: conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação;

recursos de processamento da informação: qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem;

risco: no sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

risco de segurança da informação: risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

segurança da informação: preservação da confidencialidade, integridade, disponibilidade, adicionalmente outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas;

serviços: meio de fornecimento de valor a clientes, com vistas a entregar os resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos;

SI: sigla de segurança da informação;

sistema de informação: conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada;

tecnologia da informação: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas, utilizados para obter, processar, armazenar, disseminar e fazer uso de informações; e

usuário: pessoa física ou jurídica, seja servidor público, estudante ou prestador de serviços, voluntário habilitado pela administração para acessar os ativos de informação do Incra.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 6º Esta política considera os seguintes princípios:

I - respeito aos princípios e diretrizes constitucionais, legais e regulamentares que regem a Administração Pública Federal;

II - garantia de integridade, autenticidade e disponibilidade da informação sob a custódia do Incra, com respeito ao princípio da transparência e atribuição de confidencialidade apenas nos casos expressamente previstos na legislação;

III - alinhamento estratégico da Política de Segurança da Informação - PoSIC com os demais planos institucionais;

IV - responsabilidade pelo cumprimento das normas pertinentes à segurança da informação vigentes; e

V - conscientização, educação e comunicação como alicerces fundamentais para o fomento da cultura em segurança da informação.

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 7º As diretrizes gerais constituem os pilares do controle de acesso no Incra, orientando a elaboração de norma, processo, planos, procedimentos, metodologia e ações de controle que garantem que os princípios básicos de segurança da informação sejam alcançados.

§ 1º Procedimento operacional padrão deve ser estabelecido, documentado e atualizado para implementar controles de acesso físicos e lógicos à informação e aos ativos associados à informação que são por ele gerenciados ou custodiados, com objetivo de proteger adequadamente a confidencialidade das informações não públicas, bem como a integridade e a disponibilidade das informações consideradas críticas para o negócio.

§ 2º Os controles de acesso devem ser implementados para identificação, autenticação e autorização garantindo que apenas usuários autorizados tenham acesso físico ou lógico aos recursos, sistemas ou serviços de TI.

§ 3º Rotinas devem ser configuradas para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuário, administrador e serviço para ativos e software institucionais devem ser estabelecidas e mantidas atualizadas.

§ 4º Sempre que possível controles de acesso devem ser implementados conforme necessidade legítima que justifique o acesso à informação por pessoa, sistema ou entidade, seguindo o princípio "privilégio mínimo", o qual estabelece que o perfil de acesso concedido deve incluir apenas os poderes necessários para atender as legítimas necessidades.

§ 5º Quando possível, os controles de acesso lógicos no Incra devem utilizar autenticação com certificado digital, a fim de proporcionar uma identificação inequívoca de pessoas físicas e jurídicas, assim como comprovação de autoria em transações digitais.

§ 6º Os direitos de acesso lógicos e físicos devem ser analisados criticamente, a intervalos regulares, para remover direitos que deixaram de ser necessários e para assegurar que privilégios indevidos não foram obtidos.

§ 7º Os controles de autorização, identificação e autenticação devem garantir que apenas usuários autorizados tenham acesso físico ou façam uso dos sistemas de informação do Incra.

CAPÍTULO V

ACESSO LÓGICO

Art. 8º O acesso lógico aos recursos da Rede Local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela Coordenação-Geral de Tecnologia e Gestão da Informação, baseado nas responsabilidades e tarefas de cada usuário, logo:

I - o Incra deve implementar protocolos de comunicação e redes seguros.

II - terão direito a acesso lógico aos recursos da Rede Local os usuários de recursos de tecnologia da informação.

III - para fins desta Portaria, consideram-se usuários de recursos de tecnologia da informação servidores ocupantes de cargo efetivo, temporário ou cargo em comissão, ocupantes de emprego público em exercício, assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade no Incra, que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação do Incra.

IV - o acesso remoto deve ser realizado por meio de VPN - Rede Virtual Privada, após as devidas autorizações.

V - deve ser utilizado o MFA para a autenticação de acesso remoto.

VI - o acesso a todas as aplicações corporativas ou de terceiros que estejam hospedados em fornecedores deve utilizar MFA.

VII - o Incra deve centralizar a autenticação, autorização e auditoria (AAA) dos ativos de informação da sua infraestrutura de rede.

VIII - o Incra deve adotar técnicas de segmentação de rede visando limitar o acesso de forma eficiente e segura, assegurando que apenas colaboradores e dispositivos autorizados possam interagir com partes específicas da rede.

Art. 9º O Incra deve estabelecer e manter um inventário de todas as contas gerenciadas, este deve incluir contas de usuário, administrativas, testes e serviço. Em caso de contas de serviço, o inventário deve conter no mínimo informações de:

I - área de negócio proprietária.

II - data de criação/última autorização de renovação de acesso;

III - a Coordenação-Geral de Tecnologia e Gestão da Informação é responsável por validar todas as contas ativas do órgão a cada 90 dias;

Art. 10. A Coordenação-Geral de Tecnologia e Gestão da Informação deve implementar a centralização da gestão de contas por meio de serviço de diretório e/ou identidade.

Art. 11. A Coordenação-Geral de Tecnologia e Gestão da Informação deve estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, tal inventário deve ser revisado periodicamente.

Art. 12. A Coordenação-Geral de Tecnologia e Gestão da Informação deve centralizar o controle de acesso para todos os ativos de informação da organização por meio de um serviço de diretório ou provedor de SSO.

Art. 13. A Coordenação-Geral de Tecnologia e Gestão da Informação deve definir e manter o controle de acesso dos usuários baseado em funções, logo:

I - deve ser elaborada a documentação dos direitos dos acessos para cada função dentro da organização.

II - a Coordenação-Geral de Tecnologia e Gestão da Informação deverá realizar análises de controle de acesso aos ativos institucionais para validar se todos os privilégios estão autorizados para a execução de atividades de cada função, este processo deve ser repetido de forma periódica ou quando novas funções e ativos de informação forem inseridos na organização.

III - ao conceder acesso a usuários que lidam com dados pessoais, deve-se limitar, estritamente, o acesso aos sistemas que processam esses dados ao mínimo necessário para cumprir os objetivos essenciais do processamento, em conformidade com o princípio da minimização de dados. Ao atribuir ou revogar os direitos de acesso concedidos deve-se incluir:

a) verificação de que o nível de acesso concedido é apropriado às políticas de acesso, além de ser consistente com outros requisitos, tais como, segregação de funções;

b) garantia de que os direitos de acesso não estão ativados antes que o procedimento de autorização esteja completo;

c) manutenção de um registro preciso e atualizado dos perfis dos usuários criados para os que tenham sido autorizados a acessar o sistema de informação e os dados pessoais neles contidos;

d) mudança dos direitos de acesso dos usuários que tenham mudado de função ou de atividades, e imediata remoção ou bloqueio dos direitos de acesso dos usuários que deixaram o Incra;

e) analisar criticamente os direitos de acesso em intervalos regulares;

f) analisar e aprovar, ad referendum, os pedidos de acesso a dados institucionais, por meio de APIs (Apllication Programming Interface) disponibilizadas no Conecta Gov.br, e ratificar os novos acessos no Comitê de Governança Digital - CGD e comunicar ao Comitê de Segurança da Informação e Comunicação - CSIC;

g) disponibilizar, em ferramenta própria, funcionalidade para que as unidades organizacionais, proprietárias de dados, possam avaliar e aprovar pedidos de acesso a seus respectivos dados, antes de atribuir direitos de acessos.

Art. 14. A Coordenação-Geral de Tecnologia e Gestão da Informação deve implementar um processo formal de registro de usuários que tratem de dados pessoais para permitir atribuição de direitos de acesso e fornecer medidas para lidar com o comprometimento do controle de acesso do usuário, como corrupção ou comprometimento de senhas ou outros dados de registro do usuário, para tanto podem ser realizadas as seguintes ações:

I - o uso de um identificador de usuário único, para permitir relacionar os usuários com suas responsabilidades e ações;

II - o uso compartilhado de identificador de usuário somente será permitido, onde eles são necessários por razões operacionais ou de negócios e deverá ser aprovado e documentado;

III - a garantia de que o um mesmo identificador de usuário não é emitido para outros.

CAPÍTULO VI

CONTA DE ACESSO LÓGICO E SENHA

Art. 15. Para utilização das estações de trabalho do Incra, será obrigatório o uso de uma única identificação (login) e de senha de acesso, fornecidos pela Coordenação-Geral de Tecnologia e Gestão da Informação, mediante solicitação formal pelo titular da unidade do requisitante, sendo assim, fazem-se necessários:

I - o preenchimento do formulário de solicitação de acesso se encontra disponível no Sistema Eletrônico de Informações - SEI;

II - a definição, pela unidade requisitante ao qual o usuário está vinculado, os privilégios de acesso dos usuários à Rede Local, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

III - na necessidade de utilização de perfil diferente do disponibilizado, o titular da unidade do usuário deverá encaminhar solicitação para a Coordenação-Geral de Tecnologia e Gestão da Informação, que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Art. 16. O login e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pela Coordenação-Geral de Tecnologia e Gestão da Informação quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo titular da unidade do requisitante.

Art. 17. O padrão adotado para o formato da conta de acesso do usuário é a sequência primeiro nome + ponto + último nome do usuário, como por exemplo, joao.silva.

Parágrafo único. Nos casos de já existência de conta de acesso para outro usuário, a Coordenação-Geral de Tecnologia e Gestão da Informação realizará outra combinação utilizando o nome completo do usuário para o qual a conta está sendo criada.

Art. 18. O padrão adotado para o formato da senha é o definido pela Coordenação-Geral de Tecnologia e Gestão da Informação, que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores, sendo assim:

I - a formação da senha da identificação (login) de acesso à Rede Local deve seguir as regras de:

a) possuir tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras e números, para contas que utilizam MFA e 14 (catorze) caracteres para contas que não utilizam MFA;

b) recomenda-se a utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &,...);

c) não ser formada por sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações;

d) não utilizar termos óbvios, tais como: Brasil, senha, usuário, password ou system;

e) não reutilizar as últimas 05 (cinco) senhas.

II - a Coordenação-Geral de Tecnologia e Gestão da Informação fornecerá uma senha temporária para cada conta de acesso criada no momento da liberação dessa conta e a mesma deverá ser alterada pelo usuário quando do primeiro acesso à Rede Local.

Art. 19. As senhas de acesso serão renovadas a cada 90 dias, devendo o usuário ser informado antecipadamente, a fim de que ele próprio efetue a mudança.

Parágrafo único. Caso não efetue a troca no prazo estabelecido, será bloqueado seu acesso à Rede Local até que a nova senha seja configurada.

CAPÍTULO VII

BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

Art. 20. A conta de acesso será bloqueada nos seguintes casos:

I - após 5 tentativas consecutivas de acesso errado;

II - solicitação do superior imediato do usuário com a devida justificativa;

III - quando da suspeita de mau uso dos serviços disponibilizados pelo Incra ou descumprimento da Política de Segurança da Informação - PoSIC e normas correlatas em vigência;

IV - após 90 dias consecutivos sem movimentação pelo usuário.

Art. 21. O desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do superior imediato do usuário à Coordenação-Geral de Tecnologia e Gestão da Informação.

Art. 22. Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato ou da unidade de Recursos Humanos.

Art. 23. A conta de acesso não utilizada há mais de 180 dias poderá ser cancelada.

Art. 24. O Incra deve garantir a implementação de um processo formal de cancelamento de usuários que administrem ou operem sistemas e serviços que tratem de dados pessoais. Tal processo deverá incluir:

I - a imediata remoção ou desabilitação de usuário que tenha deixado o Incra;

II - a remoção e identificação, de forma periódica, ou a desabilitação de usuários com os mesmos identificadores.

Art. 25. A Coordenação-Geral de Tecnologia e Gestão da Informação deve configurar o bloqueio automático de sessão nos ativos após um período de inatividade preestabelecido. Tal prazo pode ser específico para cada tipo de ativo.

Art. 26. A Coordenação-Geral de Tecnologia e Gestão da Informação deve, sempre que possível, priorizar a revogação/desativação de contas com o objetivo de manter dados e logs para possíveis auditorias.

CAPÍTULO VIII

ACESSO FÍSICO

Art. 27. O Incra deve definir perímetros de segurança para proteger ambientes e ativos contra acesso físico não autorizado, danos e interferências de acordo com as diretrizes a seguir:

I - definir a localização e resistência dos perímetros de acordo com os requisitos de segurança da informação relacionados aos ativos que se encontre dentro dos perímetros;

II - proteger os ambientes seguros contra acessos não autorizados por meio de mecanismos de controle de acesso, como fechaduras tradicionais ou digitais, que possibilitem autenticação por biometria, senhas, PINs ou cartões de acesso. Sendo assim:

a) o Incra deve executar testes nos mecanismos de controle de acesso em períodos pré-definidos para assegurar a funcionalidade total do equipamento;

b) os mecanismos de controle de acesso devem ser monitorados pela Coordenação-Geral de Tecnologia e Gestão da Informação.

III - estabelecer uma área de recepção ou outros meios de controle de acesso físico a ambientes que não for conveniente a implementação de mecanismos de controle de acesso.

Art. 28. O acesso físico a ambientes seguros ou ativos de tratamento e armazenamento de dados do Incra é destinado apenas a pessoal autorizado.

Art. 29. O Incra deve manter um processo de gestão de acessos para fornecimento, revisão periódica, atualização e revogação das autorizações.

Art. 30. O Incra deve implementar e manter seguro logs ou registro físico de todos os acessos aos ativos de informação.

Art. 31. O acesso a ambientes seguros ou ativos de tratamento e armazenamento de dados por fornecedores ou prestadores de serviços será concedido somente quando necessário e de acordo com as seguintes diretrizes:

I - para fins específicos e autorizados;

II - autorização concedida pela Coordenação-Geral de Tecnologia e Gestão da Informação;

III - supervisionado e monitorado.

Art. 32. Os ativos de armazenamento e tratamento de dados que se encontrem fora do Incra devem ser protegidos contra perda, roubos, danos e acesso físico não autorizados conforme as seguintes diretrizes:

I - não deixar o ativo sem vigilância em locais públicos e inseguros;

II - proteger o ativo contra riscos associados a visualização de informações por outra pessoa;

III - implementar as funcionalidades de rastreamento e limpeza remota.

Art. 33. O Incra deve estabelecer uma política ou normativo equivalente sobre a gestão de mídias de armazenamento, de acordo com as seguintes diretrizes:

I - exigir autorização para a saída de mídias de armazenamento do Incra;

II - armazenar mídias em local seguro de acordo com a classificação de suas informações;

III - criptografar as mídias de acordo com a classificação de suas informações;

IV - manter cópias de segurança de mídias de acordo com a classificação de suas informações.

Art. 34. O Incra deve elaborar política, ou normativo equivalente, que defina condições e restrições pertinentes ao acesso físico nos dispositivos de trabalho remoto, levando em consideração as seguintes diretrizes:

I - segurança física do local de trabalho remoto;

II - regras e orientações quanto ao acesso de familiares e visitantes ao dispositivo.

CAPÍTULO IX

MOVIMENTAÇÃO INTERNA

Art. 35. Quando houver mudança do usuário para outra unidade ou o usuário ocupar uma nova função, os direitos de acesso à Rede Local devem ser revogados, sendo que:

I - o novo superior imediato deve realizar a solicitação de novos acessos de acordo com nova unidade/função do usuário;

II - os direitos de acesso antigos devem ser imediatamente cancelados, conforme solicitação do antigo superior imediato.

CAPÍTULO X

CONTA DE ACESSO BIOMÉTRICO

Art. 36. A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para se obter um acesso, a fim de atender os conceitos da autenticação de multifatores (MFA).

Parágrafo único. O Incra deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO XI

ADMINISTRADORES

Art. 37. A utilização de identificação (login) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação. Sendo que:

I - somente os técnicos da Coordenação-Geral de Tecnologia e Gestão da Informação, devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede;

II - na necessidade de utilização de login com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para a Coordenação-Geral de Tecnologia e Gestão da Informação, que poderá negar os casos em que entender desnecessária a utilização;

III - se concedida a permissão ao usuário como administrador local na estação de trabalho, esse será responsável por manter a integridade da máquina, não podendo instalar, desinstalar ou remover qualquer programa sem autorização formal da Coordenação-Geral de Tecnologia e Gestão da Informação;

IV - caso constatada a irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão;

V - a identificação (login) com privilégio de administrador nos equipamentos locais será fornecida em caráter provisório, podendo ser renovada por solicitação formal do titular da unidade requisitante;

VI - salvo para atividades específicas da área responsável pela gestão da tecnologia da informação do órgão, não será concedida, para um mesmo usuário, identificação (login) com privilégio de administrador para mais de uma estação de trabalho, ou para acesso a equipamentos servidores e a dispositivos de rede;

VII - excepcionalmente, poderão ser concedidas identificações (login) de acesso à rede de comunicação de dados a visitante em caráter temporário após apreciação do superior imediato, por meio do Recursos Humanos;

VIII - a Coordenação-Geral de Tecnologia e Gestão da Informação deve implementar o MFA para todas as contas de administrador;

IX - a Coordenação-Geral de Tecnologia e Gestão da Informação deve restringir os privilégios de administrador a contas de administrador dedicados nos ativos de informação, para que o usuário com privilégio de administrador não consiga realizar atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, estas atividades deverão ser realizadas preferencialmente a partir da conta primária não privilegiada do usuário;

X - ao tratar dados pessoais a Coordenação-Geral de Tecnologia e Gestão da Informação observar o princípio do privilégio mínimo como regra, para garantir que o usuário receba apenas os direitos mínimos necessários para executar suas atividades, para tanto podem ser realizadas as seguintes ações:

a) remover os direitos de administrador nos dispositivos finais;

b) remover todos os direitos de acesso root e admin aos servidores e utilizar tecnologias que permitam a elevação granular de privilégios conforme a necessidade, ao mesmo tempo em que fornecem recursos claros de auditoria e monitoramento;

c) eliminar privilégios permanentes (privilégios que estão "sempre ativos") sempre que possível;

d) limitar a associação de uma conta privilegiada ao menor número possível de pessoas;

e) minimizar o número de direitos para cada conta privilegiada.

CAPÍTULO XII

RESPONSABILIDADES

Art. 38. É de responsabilidade do superior imediato do usuário comunicar formalmente aos Recursos Humano e à Coordenação-Geral de Tecnologia e Gestão da Informação o desligamento ou saída do usuário do Incra, para que as permissões de acesso à Rede Local sejam canceladas.

Art. 39. Caberá aos Recursos Humanos do Incra a criação, desbloqueio e revogação de permissões de acesso aos recursos via automação.

Art. 40. É responsabilidade dos Recursos Humanos do Incra a comunicação imediata à Coordenação-Geral de Tecnologia e Gestão da Informação sobre desligamentos, férias e licenças de funcionários de empresas prestadoras de serviços, para que seja efetuado o bloqueio momentâneo ou revogação definitiva da permissão de acesso aos recursos. Ademais:

I - os serviços serão filtrados por programas de antivírus, anti-phishing e anti-spam e, caso violem alguma regra de configuração, serão bloqueados ou excluídos automaticamente;

II - nenhum usuário do Incra terá acesso ao conteúdo das informações armazenadas nos equipamentos servidores do Instituto sem autorização da unidade competente.

Art. 41. É de responsabilidade da Coordenação-Geral de Tecnologia e Gestão da Informação o monitoramento da utilização de serviços de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como bloquear, temporariamente, sem aviso prévio, a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica do Incra.

Art. 42. O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à Rede Local e a recursos de tecnologia custodiados ou de propriedade do Incra, logo:

I - o usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos;

II - a utilização simultânea da conta de acesso à Rede Local em mais de uma estação de trabalho ou notebook deve ser evitada, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica;

III - o usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à Rede Local.

Art. 43. O usuário deve informar à Coordenação-Geral de Tecnologia e Gestão da Informação qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 44. É dever de o usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a Instituição, a saber:

I - não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;

II - evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;

III - interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;

IV - não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;

V - não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

VI - utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;

VII - não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis;

VIII - assinar o Termo de Responsabilidade (Modelo - Anexo I) quanto a utilização da respectiva conta de acesso.

CAPÍTULO XIII

DISPOSIÇÕES GERAIS

Art. 45. Os incidentes que afetem a segurança das informações, assim como o descumprimento da Política de Segurança da Informação - PoSIC e Normas de Segurança, devem ser obrigatoriamente comunicados pelos usuários à Coordenação-Geral de Tecnologia e Gestão da Informação.

Art. 46. Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a Coordenação-Geral de Tecnologia e Gestão da Informação fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização, e considerando que:

I - nos casos em que o ator da quebra de segurança for um usuário, a Coordenação-Geral de Tecnologia e Gestão da Informação comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis;

II - ações que violem a PoSIC, ou que quebrem os controles de Segurança da Informação, serão passíveis de sansões civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente;

III - processo administrativo disciplinar específico deverá ser instaurado para apurar as ações que constituem em quebra das diretrizes impostas por esta Norma e pela PoSIC;

IV - a resolução de casos de violação/transgressões omissos nas legislações correlatas será resolvida pelo Comitê de Segurança da Informação - CSI do Incra.

Art. 47. Esta Portaria entra em vigor na data de sua publicação.

CÉSAR FERNANDO SCHIAVON ALDRIGHI

ANEXO

Modelo de Termo de Responsabilidade

SERVIÇO PÚBLICO FEDERAL

Instituto Nacional de Colonização e Reforma Agrária - Incra

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, e lotado no(a)_____deste Ministério, DECLARO , sob pena das sanções cabíveis nos termos da _____ (legislação vigente) que assumo a responsabilidade por:

I - tratar o(s) ativo(s) de informação como patrimônio do Instituto Nacional de Colonização e Reforma Agrária - Incra;

II - utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do Incra;

III - contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 27 de maio de 2020, que Dispõe sobre Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal;

IV - utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do Incra;

V - responder, perante o Incra pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

VI - acessar a rede corporativa, computadores, Internet e/ou utilização de e-mail, somente com autorização (usuário/senha), por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail;

VII - utilizar o correio eletrônico (e-mail) colocado a minha disposição somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail;

VIII - não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

IX - manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

X - não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador (browser), bloquear estação de trabalho, bem como encerrar a seção do cliente de correio, garantindo assim a impossibilidade de acesso indevido por terceiros;

XI - não revelar minha senha de acesso à rede corporativa, computadores, Internet e/ou do correio eletrônico (e-mail) a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

XII - responder em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

<<Local>>, <<UF>>, <<dia>> de <<mês >> de <<ano>>.

Assinaturas
Nome do usuário Unidade organizacional
Nome da autoridade responsável pela autorização do acesso Unidade organizacional

Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome

CONSELHO NACIONAL DE ASSISTÊNCIA SOCIAL

RETIFICAÇÃO

No calendário de reuniões do CNAS, mês de janeiro, na Resolução CNAS/MDS nº 216, de 17 de novembro de 2025, publicada na Seção I do Diário Oficial da União de 19 de novembro de 2025, página 69, onde se lê: Dias 2 a 6 - Pedidos Habilitação Eleição CNAS, leia-se: Dias 02/01 a 06/02 - Pedidos Habilitação Eleição CNAS.

Ministério do Desenvolvimento, Indústria, Comércio e Serviços

INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA

PORTARIA Nº 849, DE 15 DE DEZEMBRO DE 2025 (*)

Aprova o Plano Diretor de Tecnologia da informação e Comunicações (PDTIC) do Inmetro, para o período 2025-2027.

O PRESIDENTE DO INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA - Inmetro, no exercício da competência que lhe foi outorgada pelos artigos 4º, § 2º, da Lei nº 5.966, de 11 de dezembro de 1973, combinado com o disposto nos artigos 18, inciso V, do Anexo I ao Decreto nº 11.221, de 05 de outubro de 2022, e 105, inciso V, do Anexo à Portaria nº 2, de 4 de janeiro de 2017, do então Ministério da Indústria, Comércio Exterior e Serviços,

Considerando a Estratégia Federal de Governo Digital para o período de 2024 a 2027, instituída pelo Decreto nº 12.198, de 24 de setembro de 2024;

Considerando a Portaria Nº 778, de 4 de abril de 2019, alterada pela Portaria n° 18.152, de 4 de agosto de 2020, que dispõe sobre a implantação da Governança de Tecnologia da Informação e Comunicação nos órgãos e entidades pertencentes ao Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal - SISP;

Considerando o que consta no Processo SEI nº 0052600.010586/2020-15; resolve:

Art. 1º Aprovar o Plano Diretor de Tecnologia da informação e Comunicações (PDTIC) do Inmetro, para o período 2025-2027, conforme deliberado em reunião do Comitê de Governança Digital em 10 de dezembro de 2025.

Art. 3º O PDTIC poderá ser revisto, sempre que necessário, a fim de assegurar seu alinhamento às prioridades e estratégias institucionais, à disponibilidade financeira e orçamentária e às mudanças na legislação pertinente.

Art. 4º Esta Portaria entra em vigor na data de sua publicação no Diário Oficial da União.

MARCIO ANDRE OLIVEIRA BRITO

(*) Republicada por ter saído, no DOU nº 749, de 16-12-2025, Seção 1, pág. 41, com incorreção no original.

Ministério dos Direitos Humanos e da Cidadania

ASSESSORIA ESPECIAL DE DEFESA DA DEMOCRACIA, MEMÓRIA E VERDADE

COORDENAÇÃO-GERAL DA COMISSÃO DE ANISTIA

PORTARIA Nº 22, DE 12 DE DEZEMBRO DE 2025

O COORDENADOR-GERAL DA COMISSÃO DE ANISTIA, no uso da competência delegada pela Portaria nº 1.817, de outubro de 2025, publicada no Diário Oficial da União, seção 1, nº 201, em 21 de outubro de 2025, para Instauração do Processo Administrativo que trata o art. 3º da Instrução Normativa nº 2, de 29 de setembro de 2021, publicada no Diário Oficial da União, seção 1, em 30 de setembro de 2021, e tendo em vista o disposto no acórdão proferido pelo Supremo Tribunal Federal no julgamento do Recurso Extraordinário nº 817.338, bem como os precedentes do Superior Tribunal de Justiça nos Mandados de Segurança nº 26.577; nº 26.496; nº 26.777 e, ainda, o constante na Nota Técnica nº 169/2025/CGGA/CA/ADMV/GM.MDHC/MDHC, de 12 de dezembro de 2025, e no Requerimento de Anistia nº 2002.01.10571, resolve:

Art. 1º Instaurar Procedimento de Revisão da Portaria nº 2.142, de 9 de dezembro de 2003, publicada no Diário Oficial da União nº 240, Seção 1, pág. 48, de 10 de dezembro de 2003, que declarou anistiado político MOISES GONÇALVES PEREIRA post mortem, filho de MARIA ALICE GONÇALVES PEREIRA, e os demais atos dela decorrentes.

Art. 2º Designar ROBERTA CAMINEIRO BAGGIO, como Conselheira-Relatora do procedimento de revisão, nos termos do §1º, do art. 3º, da Instrução Normativa nº 2, de 29 de setembro de 2021.

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

VINICIUS DE LARA RIBAS

PORTARIA Nº 23, DE 12 DE DEZEMBRO DE 2025

O COORDENADOR-GERAL DA COMISSÃO DE ANISTIA, no uso da competência delegada pela Portaria nº 1.817, de outubro de 2025, publicada no Diário Oficial da União, seção 1, nº 201, em 21 de outubro de 2025, para Instauração do Processo Administrativo que trata o art. 3º da Instrução Normativa nº 2, de 29 de setembro de 2021, publicada no Diário Oficial da União, seção 1, em 30 de setembro de 2021, e tendo em vista o disposto no acórdão proferido pelo Supremo Tribunal Federal no julgamento do Recurso Extraordinário nº 817.338, bem como os precedentes do Superior Tribunal de Justiça nos Mandados de Segurança nº 26.577; nº 26.496; nº 26.777 e, ainda, o constante na Nota Técnica nº 142/2025/CGGA/CA/ADMV/GM.MDHC/MDHC, de 12 de dezembro de 2025, e no Requerimento de Anistia nº 2003.01.23420, resolve:

Art. 1º Instaurar Procedimento de Revisão da Portaria nº 298, de 8 de março de 2005, publicada no Diário Oficial da União nº 48, Seção 1, pág. 43, de 11 de março de 2005, que declarou anistiado político JAYME SARMENTO post mortem, filho de ZILDA BALESTRASSI SARMENTO, e os demais atos dela decorrentes.

Art. 2º Designar PRUDENTE JOSE SILVEIRA MELLO, como Conselheiro-Relator do procedimento de revisão, nos termos do §1º, do art. 3º, da Instrução Normativa nº 2, de 29 de setembro de 2021.

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

VINICIUS DE LARA RIBAS

PORTARIA Nº 24, DE 12 DE DEZEMBRO DE 2025

O COORDENADOR-GERAL DA COMISSÃO DE ANISTIA, no uso da competência delegada pela Portaria nº 1.817, de outubro de 2025, publicada no Diário Oficial da União, seção 1, nº 201, em 21 de outubro de 2025, para Instauração do Processo Administrativo que trata o art. 3º da Instrução Normativa nº 2, de 29 de setembro de 2021, publicada no Diário Oficial da União, seção 1, em 30 de setembro de 2021, e tendo em vista o disposto no acórdão proferido pelo Supremo Tribunal Federal no julgamento do Recurso Extraordinário nº 817.338, bem como os precedentes do Superior Tribunal de Justiça nos Mandados de Segurança nº 26.577; nº 26.496; nº 26.777 e, ainda, o constante na Nota Técnica nº 167/2025/CGGA/CA/ADMV/GM.MDHC/MDHC, de 12 de dezembro de 2025, e no Requerimento de Anistia nº 2004.01.46070, resolve:

Art. 1º Instaurar Procedimento de Revisão da Portaria nº 1.658, de 22 de agosto de 2005, publicada no Diário Oficial da União nº 162, Seção 1, pág. 39, de 23 de agosto de 2005, que declarou anistiado político JOSE LIMEIRA DA SILVEIRA post mortem, filho de HILCE LIMEIRA DA SILVEIRA, e os demais atos dela decorrentes.

Art. 2º Designar MARINA DA SILVA STEINBRUCH, como Conselheira-Relatora do procedimento de revisão, nos termos do §1º, do art. 3º, da Instrução Normativa nº 2, de 29 de setembro de 2021.

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

VINICIUS DE LARA RIBAS

PORTARIA Nº 25, DE 12 DE DEZEMBRO DE 2025

O COORDENADOR-GERAL DA COMISSÃO DE ANISTIA, no uso da competência delegada pela Portaria nº 1.817, de outubro de 2025, publicada no Diário Oficial da União, seção 1, nº 201, em 21 de outubro de 2025, para Instauração do Processo Administrativo que trata o art. 3º da Instrução Normativa nº 2, de 29 de setembro de 2021, publicada no Diário Oficial da União, seção 1, em 30 de setembro de 2021, e tendo em vista o disposto no acórdão proferido pelo Supremo Tribunal Federal no julgamento do Recurso Extraordinário nº 817.338, bem como os precedentes do Superior Tribunal de Justiça nos Mandados de Segurança nº 26.577; nº 26.496; nº 26.777 e, ainda, o constante na Nota Técnica nº 166/2025/CGGA/CA/ADMV/GM.MDHC/MDHC, de 12 de dezembro de 2025, e no Requerimento de Anistia nº 2001.01.05299, resolve:

Art. 1º Instaurar Procedimento de Revisão da Portaria nº 1.771, de 5 de dezembro de 2002, publicada no Diário Oficial da União nº 236, Seção 1, pág. 29, de 6 de dezembro de 2002, que declarou anistiado político ACLAIR BRAZ DE ALMEIDA, inscrito no CPF nº XXX.940.497-XX, e os demais atos dela decorrentes.

Art. 2º Designar MARCELO RIBEIRO UCHOA, como Conselheiro-Relator do procedimento de revisão, nos termos do §1º, do art. 3º, da Instrução Normativa nº 2, de 29 de setembro de 2021.

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

VINICIUS DE LARA RIBAS

PORTARIA Nº 26, DE 12 DE DEZEMBRO DE 2025

O COORDENADOR-GERAL DA COMISSÃO DE ANISTIA, no uso da competência delegada pela Portaria nº 1.817, de outubro de 2025, publicada no Diário Oficial da União, seção 1, nº 201, em 21 de outubro de 2025, para Instauração do Processo Administrativo que trata o art. 3º da Instrução Normativa nº 2, de 29 de setembro de 2021, publicada no Diário Oficial da União, seção 1, em 30 de setembro de 2021, e tendo em vista o disposto no acórdão proferido pelo Supremo Tribunal Federal no julgamento do Recurso Extraordinário nº 817.338, bem como os precedentes do Superior Tribunal de Justiça nos Mandados de Segurança nº 26.577; nº 26.496; nº 26.777 e, ainda, o constante na Nota Técnica nº 155/2025/CGGA/CA/ADMV/GM.MDHC/MDHC, de 12 de dezembro de 2025, e no Requerimento de Anistia nº 2004.01.41420, resolve:

Art. 1º Instaurar Procedimento de Revisão da Portaria nº 249, de 8 de março de 2005, publicada no Diário Oficial da União nº 47, Seção 1, pág. 56, de 10 de março de 2005, que declarou anistiado político NILO JACQUES DOS SANTOS post mortem, filho de INOCENCIA DOS SANTOS, e os demais atos dela decorrentes.

Art. 2º Designar MANOEL SEVERINO MORAES DE ALMEIDA, como Conselheiro-Relator do procedimento de revisão, nos termos do §1º, do art. 3º, da Instrução Normativa nº 2, de 29 de setembro de 2021.

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

VINICIUS DE LARA RIBAS