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;