**INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA**

# PORTARIA Nº 1460, DE 15 DE JULHO DE 2022

Institui a Política de Segurança da Informação e Comunicações, no âmbito do Instituto Nacional de Colonização e Reforma Agraria - Incra.

O PRESIDENTE DO INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA - INCRA, no uso das atribuições que lhe foram conferidas pelo art. 19 da Estrutura Regimental aprovada pelo Decreto nº 10.252, de 20 de fevereiro de 2020, combinado com o art. 110, XX, do Regimento Interno da autarquia, considerando o disposto no art. 23 da Instrução Normativa Conjunta do Ministério do Planejamento, Desenvolvimento e Gestão e do Ministério da Transparência e Controladoria- Geral da União - MP/CGU nº 01, de 10 de maio de 2016, e os autos dos processos administrativos nº 54000.040337/2020-31 e nº 54000.018337/2022-16, resolve:

## CAPÍTULO I

## DO OBJETO E DA APLICAÇÃO

Art. 1º Fica instituída a Política de Segurança da Informação e Comunicações do Incra - PoSIC, para estabelecer diretrizes, regras e padrões para manuseio, tratamento, controle e proteção contra a indisponibilidade, a divulgação, a modificação e o acesso não autorizado a dados e informações.

Art. 2º Esta PoSIC aplica-se aos recursos de Tecnologia da Informação e Comunicações - TIC, ambientes e processos de trabalho, estabelecendo responsabilidades e obrigações a todos os agentes públicos que tenham acesso às informações ou aos recursos de Tecnologia da Informação - TI.

Parágrafo único. A PoSIC/Incra aplica-se tanto no ambiente informatizado quanto nos meios convencionais de processamento, comunicações e armazenamento da informação.

## CAPÍTULO II

## DAS DIRETRIZES, PRINCÍPIOS E CONCEITOS

Art. 3º As diretrizes que orientam as ações de Segurança da Informação e Comunicação - SIC do Incra visam a garantir os princípios básicos de sustentação da segurança, quais sejam, a disponibilidade, a integridade e a confidencialidade.

Art. 4º A Segurança da Informação e Comunicação no Incra está apoiada nos seguintes

processos:

I - gestão de incidentes;

II - gestão dos ativos de informação;

III - programa de capacitação e conscientização em SIC;

IV - gestão de risco e de vulnerabilidades de SIC; e

V - gestão de Continuidade dos serviços.

Parágrafo único. Os agentes públicos que tenham acesso a informações do Incra sujeitam-se às diretrizes e objetivos de segurança da informação desta PoSIC, e são responsáveis por garantir a segurança das informações a que tenham acesso.

Art. 5º Para fins desta Portaria, entende-se por:

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;

II - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

III - ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

IV - ativo: qualquer coisa que tenha valor para a organização;

V - ativos de informação: os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;

VI - Comitê de Segurança da Informação e Comunicações - CSIC/Incra: Colegiado criado pela Portaria Incra nº 825, de 28 de abril de 2020, com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do Incra;

VII - criticidade: grau de importância da informação;

VIII - equipe de prevenção, tratamento e resposta a incidentes em redes computacionais - ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores; VII - gestor de área: responsável pela área funcional onde a informação é criada, comunicada, manuseada, armazenada, custodiada, transportadas ou descartadas;

IX - gestor de segurança da informação: servidor responsável pelas ações de segurança da informação no âmbito deste órgão;

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

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

XII - política de segurança da informação - PoSIC: conjunto de procedimentos criados por meio desta Portaria, que tem como objetivo fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

XIII - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

XIV - recursos de TI: recursos de tecnologia da informação que processam, armazenam e

transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;

XV - termo de responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

XVI - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

Art. 6º As ações relacionadas com a Segurança da Informação e Comunicações no Incra são norteadas pelos seguintes princípios:

I - autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

II - celeridade: as ações de segurança da informação oferecem respostas rápidas a incidentes e falhas;

III - clareza: as regras de segurança dos ativos de segurança da informação e comunicações são precisas, concisas e de fácil entendimento;

IV - confidencialidade: as informações somente estarão disponíveis ou reveladas à pessoa, sistema, órgão ou entidade autorizada e credenciada;

V - disponibilidade: as informações estarão disponíveis e utilizável a quem dela necessita e possua autorização para acessá-la;

VI - equanimidade: as normas e regras de segurança da informação são obedecidas por todos, sem distinção de cargo ou função;

VII - ética: os direitos dos agentes públicos são preservados sem comprometimento da segurança da informação e comunicações;

VIII - finalidade: as normas e regras de segurança da informação consideram a finalidade dos ativos e das informações a que se referirem;

IX - integridade: as informações não são modificadas ou destruídas de maneira não autorizada ou acidental;

X - menor privilégio: restringir o acesso às informações, ao estritamente necessário ao exercício das funções;

XI - privacidade: informação que fira o respeito, à intimidade, à integridade e a honra dos cidadãos não podem ser divulgadas;

XII - publicidade: dar transparência no trato das informações, observado os critérios legais. Divulgar a todos os agentes públicos do Incra as diretrizes e a normas de segurança da informação; e

XIII - responsabilidade/e obediência: os agentes públicos têm o dever de conhecer e respeitar todas as normas de segurança da informação e comunicações do Incra.

Art. 7º São diretrizes gerais da Política de Segurança da Informação e Comunicações do Incra - PoSIC:

I - compromisso da alta-gestão em garantir recursos e o estabelecimento dos processos necessários a organização e sustentação da SIC;

II - dever do agente público do Incra conhecer e cumprir a PoSIC/Incra;

III - é condição para acesso aos ativos de informação do Incra a realização do Curso Básico de Segurança da Informação e a adesão formal aos termos desta Portaria, mediante assinatura de Termo

de Responsabilidade;

IV - todos os agentes públicos do Incra são responsáveis pela segurança dos ativos de informação e comunicações que estejam sob a sua responsabilidade e por todos os atos executados com suas identificações, tais como: identificação de usuário da rede - **Login**, crachá, carimbo, endereço de correio eletrônico ou assinatura digital;

V - os recursos de TI disponibilizados pelo Incra devem ser utilizados estritamente dentro do seu propósito que é a prestação do serviço público com foco na missão institucional;

VI - os contratos de prestação de serviços, firmados pelo Incra conterão cláusula específica sobre a obrigatoriedade de atendimento às diretrizes da PoSIC/Incra, devendo ainda, exigir da entidade contratada, a assinatura de Termo de Confidencialidade e o compromisso de seus colaboradores em cumprir as normas institucionais do Incra.

Art. 8º Por Propriedade Intelectual dos Ativos de Informação, deve ser entendida toda informação criada, armazenada, transportada ou descartada, incluindo o desenvolvimento de sistemas, programas e aplicações.

§ 1º A propriedade intelectual referida no **caput** é de domínio do Incra e está protegida segundo as diretrizes descritas na PoSIC/Incra e nas regulamentações em vigor.

§ 2º Na concessão de acesso e cessão de bases de dados nominais, informação custodiada ou de propriedade do Incra a terceiros, o proprietário da Informação providenciará a documentação formal relativa à cessão e um ambiente controlado e seguro para o acesso às informações, mediante autorização, antes da sua disponibilização, conforme preconiza a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados - LGPD;

§ 3º Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deverá, se necessário, providenciar junto à concedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

Art. 9º Compreende-se como tratamento da Informação, o processo pelo qual toda informação criada, manuseada, armazenada, transportada, descartada ou custodiada pelo Incra, cuja responsabilidade é dos agentes públicos, devem ser classificadas e protegidas adequadamente, quanto aos aspectos de confidencialidade, integridade, autenticidade e disponibilidade, de forma explícita ou implícita conforme o Decreto nº 7.845, de 14 de novembro de 2012.

§ 1º O tratamento referente aos dados pessoais deverá atender ao disposto na LGPD e ser monitorado pelo Encarregado pelo Tratamento dos Dados Pessoais no Incra;

§ 2º A classificação da informação é atribuição do dono da Informação e será feito na forma da legislação aplicável.

§ 3º Toda informação institucional eletrônica e bases de dados estarão armazenadas de forma segura, controlada e protegida nos servidores de arquivo sob gestão e administração da área de TIC ou em servidores de nuvem contratados pelo Incra. As informações não eletrônicas serão mantidas em local que as salvaguarde adequadamente.

§ 4º Toda informação institucional, sob a forma eletrônica, estará salvaguardada por meio de retenção, cópia física de segurança ou em servidores em nuvem. Seu armazenamento é de responsabilidade da área de TIC, que deverá manter em local seguro, controlado e protegido que garanta sua recuperação em caso de perda da informação original.

§ 5º No descarte de informações institucionais serão observadas as políticas, normas, procedimentos internos, a classificação que a informação possui, bem como a temporalidade prevista na legislação e serão adotas medidas técnicas para impedir que as informações sejam recuperadas novamente;

§ 6º As informações classificadas conforme a legislação vigente, produzidas, armazenadas

e transportadas em meios eletrônicos, utilizarão criptografia compatível com o grau de sigilo, em especial as informações de autenticação dos usuários das aplicações.

## CAPÍTULO III

## DAS DISPOSIÇÕES GERAIS

Art. 10. Fica estabelecido o Processo de Gestão de Riscos de Segurança da Informação - PGRSI, que integrará a Política de Gestão de Riscos do Incra, com vistas a minimizar possíveis impactos associados aos ativos de informação da autarquia.

Art. 11. Fica estabelecido o Programa de Gestão de Continuidade de Negócio - PGCN, em segurança da informação no âmbito do Incra, de modo a reduzir a possibilidade de interrupção causada por desastres ou falhas nos recursos de TIC que suportam as operações do Incra.

§ 1º Todo sistema ou serviço crítico do Incra deverá estar em infraestrutura dedicada de alta disponibilidade e ser suportado pelo PGCN.

§ 2º Os sistemas institucionais devem ser avaliados anualmente quanto a sua criticidade.

Art. 12. O uso dos recursos de TIC disponibilizados pelo Incra deve ser objeto amplo controle e auditoria, com a utilização de softwares específicos para o monitoramento do uso dos sistemas, bem como a implantação de mecanismos que permitam a sua rastreabilidade.

§ 1º Serão mantidos procedimentos de controle, a exemplo de trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos, para todos os sistemas corporativos da rede interna do Incra.

§ 2º Fica estabelecida a gestão de conformidade dos processos de TIC com a POSIC, normas e boas práticas de SI estabelecidas.

Art. 13. O agente público do Incra que utilizar os recursos de TIC terá uma conta de acesso, única e intransferível, cuja concessão de acesso será regulamentada em portaria específica.

§ 1º O gestor da informação, nomeado por portaria, é responsável pela concessão e revogação dos privilégios de acesso às informações, considerando sempre o princípio do menor privilégio.

§ 2º A identificação do agente público, qualquer que seja o meio e a forma, é pessoal e intransferível, devendo permitir o seu reconhecimento de maneira inequívoca.

§ 3º Compete à Coordenação-Geral de Tecnologia e Gestão da Informação o controle de senhas administrativas de sistemas críticos, seguindo as melhores práticas.

§ 4º Deverá ser utilizada ferramenta de Múltiplo Fator de Autenticação - MFA, para acesso a recursos administrativos, quando disponível.

Art. 14. O correio eletrônico do Incra é de uso exclusivo de agentes públicos no exercício de suas funções, incluindo-se servidores e demais colaboradores, e suas regras de acesso e utilização serão definidas por meio de portaria, em conformidade com a PoSIC/Incra e demais normas aplicáveis.

Art. 15. O acesso aos serviços de Internet no ambiente de trabalho do Incra está condicionado às necessidades dos agentes públicos no exercício de suas atribuições e será regido por

portaria específica, em conformidade com a PoSIC/Incra e demais normas de regência.

Parágrafo único. A liberação dos serviços de internet deverá ser aprovada pela área de TIC do Incra.

Art. 16. O processo de gestão de mudanças, no âmbito do Incra, será composto, no mínimo, pelas fases de Comunicação, Descrição, Avaliação, Aprovação, Implementação e Verificação, de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

Parágrafo único. Toda mudança no ambiente, que tenha sido homologada e testada, necessita ser documentada e registrada.

Art. 17. Para a Gestão de Ativos de Informação, fica estabelecido, no âmbito do Incra, o processo de Inventário e Mapeamento dos Ativos de Informação, objetivando a Segurança das Infraestruturas que sustentam os serviços informatizados.

Parágrafo único. O processo de Inventário e Mapeamento de Ativos de Informação subsidiará o conhecimento, valoração, proteção e manutenção de seus ativos de informação, devendo ser dinâmico, periódico e estruturado, com o objetivo de manter a base de dados sempre atualizada.

Art. 18. O uso dos dispositivos móveis portáteis por agentes públicos usuários da rede do Incra deverá ser realizado no interesse do órgão, sendo vedado o uso de dispositivos de armazenamento de mídias, seja **pendrive, hard disk,** portáteis, não confiáveis.

§ 1º Todo dispositivo móvel usado para acessar a rede corporativa do Incra estará submetido aos padrões de uso estabelecidos pela autarquia, devendo ser monitorado pela área de TIC.

§ 2º A área de TIC proverá uma rede segregada da rede corporativa para acesso à Internet pelos visitantes.

Art. 19. O ambiente de computação em nuvem, bem como sua infraestrutura e canal de comunicações, devem ser compatíveis com as diretrizes e normas de SIC estabelecidas pelo Incra e demais legislações aplicáveis.

§ 1º O uso dos serviços de computação em nuvem deverá estar amparado por contrato firmado com o Incra, de modo a garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem;

§ 2º O armazenamento de dados pessoais e sensíveis deverá estar adequadamente protegido, de modo a evitar o acesso indevido, nos termos da LGPD.

Art. 20. O uso institucional das redes sociais nos aspectos relacionados à Segurança da Informação deverá ser objeto de análise em relação a norma específica da Administração Pública Federal - APF que, além da SIC, abordará a estratégia de comunicações social, o processo de gestão de conteúdo e outros aspectos relevantes.

§ 1º A existência de portaria interna de uso seguro das redes sociais deverá estabelecer diretrizes, critérios, limitações e responsabilidades na gestão do uso seguro das redes sociais por usuários que tenham permissão para administrar perfis institucionais ou que possuam credencial de acesso para qualquer outra rede social institucional a partir da infraestrutura de rede de computadores do Incra.

§ 2º Perfis institucionais mantidos nas redes sociais devem ser administrados e gerenciados por servidor lotado na área de comunicação do Incra, ou estar sob a coordenação e

responsabilidade desta área.

§ 3º Será designado servidor público ocupante de cargo efetivo para a função de Agente Responsável pela gestão do uso seguro dos perfis institucionais da autarquia nas redes sociais.

Art. 21. O Desenvolvimento de **Software** Seguro - DSS, pressupõe a identificação dos responsáveis pela definição e validação dos requisitos de segurança que o software deva atender, observado o seguinte:

I - serão definidos e documentados os requisitos de segurança para aplicação desde o início do projeto de desenvolvimento ou aquisição de **software**;

II - será definida a execução de testes de segurança pela contratada e homologação pelo Incra antes da instalação do **software** em ambiente de produção;

III - será realizado teste de mesa do **software** desenvolvido por terceiros;

§ 1º Fica estabelecida a obrigatoriedade de análise de vulnerabilidades da aplicação, gerenciamento de monitoração da performance ponto a ponto e análise Dinâmica, antes da implantação de qualquer **software** ou aplicação, não sendo permitida a operacionalização enquanto perdurar qualquer falha de segurança considerada crítica.

§ 2º O tratamento das vulnerabilidades constitui um dos requisitos para a aceitação do sistema.

Art. 22. Para a preservação de evidências, os equipamentos servidores de rede, bem como qualquer outro ativo de informação, devem ser configurados para armazenar registros históricos de eventos - **Logs**, em formato que permita a completa identificação dos fluxos de dados e das operações de seus administradores.

Parágrafo único. Os registros devem ser armazenados pelo período mínimo de 06 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos, e os ativos de informação devem ser configurados de forma a armazenar seus registros de auditoria não apenas localmente, por meio de tecnologia aplicável, de forma a garantir sua integridade.

Art. 23. Compete à Diretoria de Gestão Operacional a Gestão da Segurança da Informação e Comunicação no âmbito do Incra.

Parágrafo único. Ao Diretor de Gestão Operacional caberá a função de Gestor de Segurança da Informação - GSI, com as seguintes atribuições:

I - promover cultura de segurança da informação e comunicações;

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III - propor recursos necessários às ações de segurança da informação e comunicações;

IV - coordenar a equipe de prevenção, tratamento e resposta a incidentes cibernéticos;

V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança das informações e comunicações;

VI - estabelecer contato direto com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações;

VII - editar as normas complementares relativas à segurança da informação e comunicações;

VIII - promover capacitações sobre Segurança da Informação e Comunicação;

IX - julgar eventuais recursos administrativos que tenham por objeto a aplicação desta Portaria.

Art. 24. O Incra promoverá ações permanentes de conscientização e de capacitação dos agentes públicos, visando a disseminação das diretrizes e normas estabelecidas nesta PoSIC.

Art. 25. Todo agente público, para acessar a rede corporativa do Incra, deverá assinar termo circunstanciado de ciência sobre a Política de Segurança da Informação da autarquia.

## CAPÍTULO IV

## DAS DISPOSIÇÕES FINAIS

Art. 26. O descumprimento do disposto nesta PoSIC/Incra sujeitará o infrator a sanções administrativas, cíveis e penais, conforme o caso e na forma da lei, observado o devido processo legal.

Art. 27. Os casos omissos serão dirimidos pelo Gestor de Segurança da Informação do Incra.

Art. 28. Esta Portaria entra em vigor em 1º de agosto de 2022.