INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA

PORTARIA Nº 1484, DE 18 DE JULHO DE 2022

Institui a Política de **Backup** e Recuperação de Dados Digitais, no âmbito do Instituto Nacional de Colonização e Reforma Agrária - Incra.

O DIRETOR DA DIRETORIA DE GESTÃO OPERACIONAL DO INSTITUTO NACIONAL DE COLONIZAÇÃO E REFORMA AGRÁRIA - Incra, no uso das atribuições que lhe foram conferidas pelo art. 9º da Estrutura Regimental do Incra, aprovada pelo Decreto nº 10.252, de 20 de fevereiro de 2020, combinado com o art. 113 do Regimento Interno da Autarquia, aprovado pela Portaria nº 531, de 23 de março de 2020, publicada no DOU do dia 24 seguinte, e considerando o que consta dos processos administrativos nº 54000.040337/2020-31, nº 54000.018337/2022-16 e nº 54000.018332/2022-93, resolve:

CAPÍTULO I

DO OBJETO, DA APLICAÇÃO E DOS CONCEITOS

Art. 1º Fica instituída a Política de **Backup** e Recuperação de Dados Digitais no âmbito do Incra, para estabelecer regras e procedimentos gerais de segurança para o uso dos recursos de Tecnologia da Informação, como medida integrante da Política de Segurança da Informação e Comunicações - PoSIC, de que trata a Portaria Incra nº 1.460, de 15 de julho de 2022.

Art. 2º A Política de **backup** e recuperação de dados digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados na infraestrutura de tecnologia da informação - TI do Incra.

Art. 3º A política de que trata esta Portaria se aplica a todas as unidades do Incra que tenham, sob sua custódia, dados em suporte digital.

Art. 4º O **backup** e a recuperação dos dados digitais do Incra abrangem exclusivamente dados digitais custodiados na infraestrutura de tecnologia da informação da Autarquia, cuja responsabilidade é da Coordenação-Geral de Tecnologia da Informação e Gestão da Informação.

Parágrafo único. Não serão salvaguardados, nem recuperados, dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos ou ambientes fora da infraestrutura de tecnologia da informação do Incra.

Art. 5º Todos os contratos, convênios, acordos e instrumentos congêneres cujo cumprimento do objeto produza ou manuseie dados digitais, devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta Política de **backup.**

§ 1º O **backup** dos dados em formato digital relacionados a ativos de informação do Incra, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantido nos acordos ou contratos que formalizam a relação entre os envolvidos.

§ 2º Excepcionalmente, a Coordenação-Geral de Tecnologia da Informação e Gestão da Informação poderá optar pela realização do **backup** de dados dispostos em nuvem nos **appliances on premises**, quando devidamente justificado, considerando os princípios da economicidade e da continuidade dos serviços públicos.

Art. 6º Para os fins desta Portaria, considera-se:

I - administrador de **backup**: unidade responsável pelo planejamento de soluções de **backup**, definição de padrões, configurações e atendimento avançado de resolução de incidentes e problemas referentes a **backups.**

II - Divisão de Infraestrutura de Rede e Comunicação de Dados: unidade responsável pela operação técnica dos ativos e serviços de Tecnologia da Informação - TI;

III - 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;

IV - **backup** ou cópia de segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação;

V - **backup** completo: modalidade de Backup em que todos os dados a serem salvaguardados são copiados integralmente, cópia de segurança completa, para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último **backup**;

VI - **backup** incremental: modalidade de backup em que são salvaguardados apenas os dados novos ou modificados desde o último backup de qualquer modalidade efetuado;

VII - **bakup** diferencial: modalidade de Backup em que são salvaguardados apenas dados novos ou modificados desde o último Backup completo efetuado;

VIII - criticidade: grau de importância dos dados para a continuidade das atividades e serviços da organização;

IX - descarte: eliminação correta de informações, documentos, mídias e acervos digitais;

X - disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

XI - imagem de **backup**: arquivo gerado pela solução de **backup**, não necessariamente no formato original dos arquivos que contêm os dados salvaguardados;

XII - infraestrutura de tecnologia da informação: consiste nos componentes e serviços que fornecem a base para sustentar todos os sistemas de informação de uma organização;

XIII - janela de **backup**: período durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas;

XIV - plano de **backup***:* planejamento que detalha a execução da Política de **backup**, no qual são anexadas as rotina e roteiro de **backup** de cada dado ou informação a ser salvaguardado;

XV - proprietário da informação: área interessada do órgão ou indivíduo legalmente instituído por sua posição ou cargo, que é responsável primário pela viabilidade e sobrevivência da informação;

XVI - **Recovery Point Objective (RPO):** ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente;

XVII - **Recovery Time Objective (RTO):** tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados, após um incidente;

XVIII - restauração: processo de recuperação e disponibilização de dados salvaguardados

em determinada imagem de **backup**;

XIX - retenção: período pelo qual os dados devem ser salvaguardados e estar aptos à restauração;

XX - rotina/roteiro de **backup**: procedimento utilizado para se realizar um **backup**;

XXI - serviço de TI: provimento de serviços de desenvolvimento, de implantação, de manutenção, de armazenamento e de recuperação de dados e de operação de sistemas de informação, projeto de infraestrutura de redes de comunicação de dados, modelagem de processos e assessoramento técnico necessários à gestão da informação;

XXII - unidade de armazenamento: dispositivo para armazenamento de dados em suporte digital; e

XXIII - unidade de armazenamento de **backup:** unidade de armazenamento com características específicas para retenção de cópia de segurança de dados digitais.

CAPÍTULO II

DOS PRINCÍPIOS GERAIS

Art. 7º A política de **backup** e recuperação de dados digitais deve estar alinhada a uma gestão de continuidade de serviços públicos em nível organizacional estabelecidos na Política de Segurança da Informação e Comunicações - PoSIC.

Art. 8º O plano de **backup** deve conter as rotinas de **backup** para cada serviço ou recurso que armazene dado digital, cumprindo as diretrizes da Política, definindo requisitos específicos de segurança da informação paras as cópias de segurança realizadas.

Art. 9º O plano de **backup** deve atender ao **checklist** constante no Anexo I desta Portaria.

Parágrafo único. Os pontos do **checklist** que não sejam atendidos ou não se aplicarem, devem ser devidamente justificados, considerando os princípios da economicidade e da continuidade dos serviços públicos.

Art. 10. As rotinas de **backup** devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços ou recurso.

Art. 11. As rotinas de **backup** devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço, recurso ou dado salvaguardado, dando prioridade aos serviços ou recursos críticos da organização.

Art. 12. O **backup** de serviços ou recursos não críticos devem ser formalmente solicitados ao administrador de **backup** pelo proprietário da informação.

Art. 13. As rotinas de backup dos dados referentes aos serviços e recursos críticos e não críticos devem refletir os requisitos de negócio da organização, bem como os requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização, e devem explicitar os seguintes requisitos técnicos:

I - escopo com os dados digitais a serem salvaguardados;

II - tipo de **backup** se completo, incremental, diferencial;

III - frequência temporal de realização do **backup** se diária, semanal, mensal, anual;

IV - retenção;

V - **Recovery Point Objective** - RPO;

VI - **Recovery Time Objective** - RTO;

VII - requisitos de segurança da informação; e

VIII - requisitos legais e normativos.

Parágrafo único. Os incisos I, III, IV, VII e VIII deste artigo são vinculados à segurança e criticidade da informação para a continuidade da operação da organização, razão pela qual devem ser definidos pelo proprietário da informação, com o apoio técnico do administrador de **backup.**

CAPÍTULO III

DAS FERRAMENTAS DE BACKUP

Art. 14. As rotinas de **backup** devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

Art. 15. Os ativos envolvidos no processo de **backup** são considerados ativos críticos para a organização.

Parágrafo único. Compete à Coordenação Geral de Tecnologia e Gestão da Informação solicitar, à Diretoria de Gestão Operacional - DO, com as justificativas pertinentes, os equipamentos necessários para manter o parque de ativos sempre atualizado e em quantidade necessária ao atendimento da demanda da Autarquia.

CAPÍTULO IV

DA FREQUÊNCIA E RETENÇÃO DOS DADOS

Art. 16. Os **backups** dos serviços ou recursos críticos do Incra devem ser realizados utilizando-se as seguintes frequências temporais:

I - diária;

II - semanal;

III - mensal; e

IV - anual.

Parágrafo único. Deverá ser avaliada a necessidade de realização de **backups** com frequência menor que a diária, conforme a criticidade do serviço ou recurso.

Art. 17. Os serviços ou recursos críticos do Incra devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência e retenção de dados estabelecida a seguir:

I - diária de forma diferencial, sendo o semanal **backup** completo de forma compactada;

II - semanal, sendo compactado para armazenamento mensal;

III - mensal, sendo compactado para armazenamento de 1 ano;

IV - anual, sendo compactado para armazenamento de 5 anos.

Art. 18. Os serviços e recursos não críticos do Incra devem ser resguardados observando se o padrão mínimo de correlação frequência e retenção de dados estabelecida a seguir:

I - diária de forma diferencial, sendo o semanal **backup** completo de forma compactada;

II - semanal, sendo compactado para armazenamento mensal;

III - mensal, sendo compactado para armazenamento de 6 meses;

IV - anual, sendo compactado para armazenamento de 1 ano.

Parágrafo único. No caso de suíte de escritório, por exemplo Office 365. O prazo de armazenamento de 05 anos.

Art. 19. Especificidades dos serviços ou recursos críticos e não críticos podem demandar frequência e tempo de retenção diferenciados, cabendo a devida justificativa na respectiva rotina de **backup**, acordadas entre o proprietário da informação e o administrador de **backup.**

Art. 20. A recuperação de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança.

Parágrafo único. Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de **backup.**

Art. 21. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao Administrador de **backup** e acordadas junto ao proprietário da informação.

CAPÍTULO V

DO USO DA REDE E DAS UNIDADES DE ARMAZENAMENTO

Art. 22. O administrador de **backup** deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do Incra, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços e recursos de Tecnologia da Informação do Incra.

Art. 23. . A execução do **backup** deve concentrar-se, preferencialmente, no período de janela de **backup.**

Parágrafo único. O período de janela de **backup** deve ser determinado pelo administrador de **backup** em conjunto com o proprietário da informação.

Art. 24. As unidades de armazenamento utilizadas no **backup** dos dados digitais devem considerar as seguintes características dos dados resguardados:

I - a criticidade do dado salvaguardado;

II - o tempo de retenção do dado;

III - a probabilidade de necessidade de restauração;

IV - o tempo esperado para restauração;

V - o custo de aquisição da unidade de armazenamento de **backup**; e

VI - a vida útil da unidade de armazenamento de **backup.**

Art. 25. O Administrador de **backup** deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

Art. 26. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de recuperação dos dados seja considerado aceitável pelo proprietário da informação.

Art. 27. As unidades de armazenamento dos **backups** devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade e temperatura, e com acesso restrito a pessoas autorizadas pelo administrador de **backup.**

Art. 28. Os **backups** podem ser classificados como **on-line**, **off-line** ou **off-site**, a depender da forma de acesso ao **backup** realizado:

I - **on-line** - uma vez realizado, o **backup** é acessível dentro da rede de dados do Incra;

II - **off-line** - uma vez realizado, o **backup** não é acessível em rede, sendo armazenado em mídias físicas removíveis; e

III - **off-site** - uma vez realizado, o **backup** é armazenado em outro data center, geograficamente separado, ou em serviço de backup em nuvem.

Art. 29. Preferencialmente, quando possível, os **backups** devem ter no mínimo duas cópias, realizadas em formatos de mídia distintos, sendo um **on-line** e outro **off-line** ou **off-site**.

Parágrafo único. Os dados considerados críticos devem ser armazenados no mínimo, de forma redundante, off-line e off-site..

Art. 30. **Backups** armazenados em nuvem estão sujeitos à Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais.

Art. 31. **Backups** com dados sensíveis e que requeiram tratamento específico quanto à segurança da informação devem ser criptografados e ter seus acessos devidamente controlados.

Art. 32. Observada a necessidade de descarte de unidades de armazenamento de **backups**, os recursos deverão ser fisicamente destruídos de forma a inutilizá-los, garantindo a sanitização dos dados, atentando-se ao descarte sustentável e ambientalmente correto.

CAPÍTULO VI

DOS TESTES DE RESTAURAÇÃO

Art. 33. Os **backups** devem ser testados periodicamente quanto à restauração, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

§ 1º O administrador de **backup** deverá elaborar cronograma de testagem priorizando os **backups** mais importantes para a continuidade das rotinas de trabalho por nível de criticidade (ou relevância) dos dados, aplicações e sistemas, do qual o proprietário da informação deve estar ciente e de acordo.

§ 2º A metodologia a ser utilizada para testes será o teste de **restore**.

§ 3º Realizado o **restore** com sucesso, o proprietário da informação deve providenciar os testes de validação da integridade dos dados.

§ 4º Os resultados dos testes serão adequadamente documentados.

Art. 34. Os testes de restauração dos **backups** devem ser realizados, por amostragem, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis no Incra.

Art. 35. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de **backup** serão definidos em plano de **backup**.

§ 1º A alteração das frequências da realização de testes de **backup** deve ser precedida de solicitação e justificativa formais encaminhadas ao administrador de **backup** e acordadas junto ao proprietário da informação.

§ 2º Recomenda-se que os testes de restauração, **restore**, dos **backup** dos dados críticos sejam realizados semestralmente e dos dados não críticos, anualmente.

CAPÍTULO VII

DAS RESPONSABILIDADES

Art. 36. São atribuições do administrador de **backup**:

I - propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas no Incra;

II - providenciar a criação e manutenção dos **backups**;

III - providenciar a configuração das soluções de **backup**;

IV - providenciar a manutenção das unidades de armazenamento de **backups** preservadas, funcionais e seguras;

V - providenciar a definição dos procedimentos de restauração;

VI - providenciar as medidas preventivas para evitar falhas;

VII - reportar imediatamente a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR os incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de **backups**;

VIII - providenciar a disponibilização das informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos backups;

IX - propor modificações visando ao aperfeiçoamento da Política de **backups** e Recuperação de Dados Digitais, objeto desta Instrução Normativa;

X - providenciar a execução dos testes de restauração;

XI - providenciar a elaboração dos procedimentos operacionais;

XII - providenciar a restauração ou recuperação dos **backups** em caso de necessidade, com anuência do proprietário da informação;

XIII - providenciar a operação e manuseio das unidades de armazenamento de **backups**;

XIV - providenciar o gerenciamento das mensagens e registros de auditoria (LOGs) diários dos backups;

XV - providenciar a verificação diária dos eventos gerados pela solução de **backup**, tomando as providências necessárias para remediação de eventuais falhas;

XVI - sanar dúvidas técnicas do proprietário da informação acerca das informações salvaguardadas;

XVII - providenciar a validação, tecnicamente, do resultado das restaurações eventualmente solicitadas; e

XVIII - providenciar a validação, tecnicamente, do resultado dos testes de restauração dos **backups**.

Art. 37. São atribuições dos proprietários da informação:

I - solicitar, formalmente, a salvaguarda das informações geridas;

II - providenciar a validação, negocialmente, do resultado das restaurações eventualmente solicitadas;

III - providenciar a validação, negocialmente, do resultado dos testes de restauração dos **backups**; e

IV - informar qual o escopo de dados, recursos e ou serviços serão incluídos na rotina de **backup**.

Art. 38. O administrador de **backup** terá a prerrogativa Renumerar o dispositivo. Onde houver palavras de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.

CAPÍTULO VIII

DAS DISPOSIÇÕES FINAIS

Art. 39. Os casos omissos serão dirimidos pela Coordenação-Geral de Tecnologia e Gestão

da Informação, podendo ser submetidos ao Gestor de Segurança da Informação do Incra.

Art. 40. Esta Portaria entra em vigor em 1º de agosto de 2022.

ANEXO I

CHECKLIST PARA VERIFICAÇÃO DO PLANO (OU PROCEDIMENTO/ROTEIRO) DE BACKUP

ID	VERIFICAR SE	SIM/NÃO/NÃO SE APLICA	OBSERVAÇÕES / EVIDÊNCIAS
1	O Plano está em *compliance* com as orientações de boas práticas recomendadas pelo TCU?		
2	O Plano tem previsão de teste periódico de restauração em conformidade com o Programa de Gestão de Continuidade de Negócios - PGCN?		
3	O plano foi publicado/comunicado para as partes interessadas (titulares dos dados, usuários e gestores dos sistemas etc.)?		
4	O plano foi aprovado pelas partes interessadas?		
5	O plano registra/define de modo completo e exato a abrangência/escopo das cópias de segurança (ou seja, aquilo que deve ser copiado, incluindo indicações de datas/períodos) Ex.: quais arquivos de dados ou de sistema, quais bases de dados, quais tabelas, quais pastas/folders etc?		
6	O plano estabelece que seja monitorada e documentada a execução do procedimento de geração das cópias de segurança, por meio de registros (logs) relativos a todos os itens copiados, a fim de detectar eventuais falhas e assegurar que houve a realização integral das cópias de segurança?		
7	O plano documenta os procedimentos para realizar a recuperação/restauração (restore) das cópias de segurança quando necessário (ou seja, o "como" recuperar os backups)?		
8	O plano define a frequência de realização das cópias de segurança (ex.: diária, semanal, mensal, anual etc.)?		
9	O plano define os tipos de cópias a serem realizadas (completa, incremental ou diferencial)?		
10	O plano define o tempo de retenção das cópias de segurança?		
11	O plano define requisitos específicos de segurança da informação (ex.: controles de acesso lógico, uso de criptografia etc.) e requisitos relativos à confidencialidade, à integridade e à disponibilidade das informações?		
12	O plano define a necessidade de armazenamento das cópias de segurança em local seguro e em local remoto seguro diferente do local original?		

13	O plano define procedimentos regulares de teste de recuperação/restauração (restore) das cópias de segurança, a fim de detectar tempestivamente eventuais falhas lógicas e físicas (nas mídias de armazenamento)?		
14	O plano estabelece que a execução dos procedimentos de teste de recuperação/restauração (restore) das cópias de segurança seja documentada por meio de registros (logs) relativos a todos os itens restaurados, a fim de detectar eventuais falhas e assegurar que houve a recuperação integral das informações?		
15	Foram identificados os dados que estão replicados em ambientes externos ao Incra e que possuem replicação no ambiente do Incra, por exemplo: sistemas e aplicações hospedados no SERPRO?		