MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA, COMÉRCIO E SERVIÇOS
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

INSTRUÇÃO NORMATIVA/INPI/PR Nº 01, DE 01 DE FEVEREIRO DE 2023

O DIRETOR DE ADMINISTRAÇÃO, NO EXERCÍCIO DA PRESIDÊNCIA DO INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL – INPI, no uso das atribuições que lhe conferem o Regimento Interno, aprovado por meio da Portaria do Ministério da Indústria, Comércio Exterior e Serviços (MDIC) nº 11, de 27 de janeiro de 2017, e tendo em vista o previsto na Lei Nº 13.709, de 14 de agosto de 2018; no Decreto nº 9.637, de 26 de dezembro de 2018; no Decreto nº 10.332, de 29 de abril de 2020 e na PORTARIA/INPI/PR nº 65, de 1° de setembro de 2022, assim como o constante nos autos do processo INPI nº 52402.001058/2020-01, **RESOLVE**:

Art. 1º Fica instituída a Política de Cópia de Segurança (Backup) e Restauração de Dados (Restore) no âmbito do Instituto Nacional da Propriedade Industrial (INPI).

CAPÍTULO I
DO PROPÓSITO

Art. 2º A Política de Backup e Restauração de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pelas unidades organizacionais do INPI e formalmente definidos como de necessária salvaguarda, para se manter a continuidade do negócio e assegurar sua missão institucional.

CAPÍTULO II
DO ESCOPO

Art. 3º Esta política é aplicável a todo o Instituto, devendo ser observada por todos os servidores, colaboradores, fornecedores, prestadores de serviço e por aqueles que, de alguma forma, executem atividades vinculadas à atuação institucional do INPI.

Parágrafo único. Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando nesses casos o backup sob a responsabilidade do indivíduo que usa o(s) dispositivo(s)

CAPÍTULO III
DOS CONCEITOS

Art. 4º Para efeitos desta Política são estabelecidos os seguintes conceitos:

I - Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II - Backup ou cópia de segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema ou ativo 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;

III - Comitê de Segurança da Informação: grupo de pessoas, formalmente instituído pelo INPI, com a atribuição de assessorar a implementação das ações de segurança da informação e deliberar sobre assuntos relativos à POSIN e à Política Nacional de Segurança da Informação (PNSI);

IV - Coordenação Geral de Tecnologia da Informação (CGTI): trata-se da Coordenação do INPI responsável pela área de Tecnologia da Informação;

V - Cópia de segurança ou backup completo: Modo de cópia de segurança que copia integralmente todos os arquivos ou dados selecionados;

VI - Cópia de segurança ou backup incremental: Modo de cópia de segurança que copia somente os arquivos ou dados criados ou alterados após a realização da última cópia de segurança;

VII - Cópia de segurança ou backup diferencial: modo de cópia de segurança que copia somente os dados que mudaram ou foram criados depois do último backup completo salvos;

VIII - Gestor de Segurança da Informação: responsável pelas ações de segurança da informação no âmbito do INPI;

IX - Mídia: meio físico no qual as informações de cópia de segurança são efetivamente armazenadas;

X - Retenção: período de tempo em que o conteúdo das cópias de segurança deverá ser preservado na mídia;

XI - Servidor: computador de alta capacidade que faz parte de uma rede coorporativa e que fornece serviços a outros computadores;

XII - Servidor de arquivos: servidor onde são armazenados os arquivos corporativos;

XIII - Restore: restauração dos dados de um backup, quando existe a necessidade de recuperá-los;

XIV - 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; e

XV - 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.

CAPÍTULO IV
DOS PRINCÍPIOS GERAIS

Art. 5º A Política de Backup e Restauração de Dados está alinhada com a Política de Segurança da Informação do INPI (POSIN-INPI), e com a gestão de continuidade de negócios em nível organizacional.

Art. 6° As rotinas de backup devem ser estabelecidas com o objetivo de restaurar os dados 3 no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

Art. 7° Os sistemas de backup devem utilizar, preferencialmente, soluções próprias e especializadas para este fim, de forma automatizada.

Art. 8° As rotinas de backup devem possuir requisitos mínimos diferenciados, de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI considerados críticos pelo INPI.

Art. 9° Se possível, a infraestrutura da solução de backup deve ser segregada, lógica e/ou fisicamente, dos sistemas críticos. E, uma reserva de recursos (físicos e lógicos) de infraestrutura deve ser estabelecida para realização de teste de restauração de backup.

Art. 10 As cópias de segurança poderão ser protegidas por encriptação quando houver necessidade de confidencialidade.

CAPÍTULO V
DOS BACKUPS, CLASSIFICAÇÃO E PERIODICIDADE

Art. 11 A definição da estratégia e da periodicidade do backup deve estar baseada no entendimento da aplicação, do seu ciclo de operação, do volume de dados e do nível de criticidade das informações custodeadas.

Art. 12 A frequência, o tempo para realização, o modo e o tempo de retenção das cópias de segurança deverão obedecer às seguintes orientações:

I - Cópia de segurança diária: realizada de segunda-feira a quinta-feira; início às 0 h e conclusão até as 8 h; de modo incremental; com retenção dos dezesseis últimos dias.

II - Cópia de segurança mensal: realizada na primeira sexta-feira do mês; início às 20 h de sexta-feira e conclusão até as 8 h de segunda-feira; de modo completo; com retenção dos doze últimos meses.

III - Cópia de segurança anual: realizada toda primeira sexta-feira do mês de janeiro; início às 20 h de sexta-feira e conclusão até as 8 h de segunda-feira; de modo completo; com retenção dos cinco últimos anos.

§ 1º No caso de erro na cópia de segurança, após a identificação e tratamento da causa do erro, o procedimento será refeito a partir da primeira hora útil após a solução efetiva.

§ 2º No caso de falha em arquivos ou diretórios da cópia de segurança, o administrador do backup receberá um alerta informando o ativo de informação, a hora de início e de término, os objetos que apresentaram falha e a respectiva razão.

§ 3º Após analisar e solucionar a falha, o administrador do backup poderá solicitar uma nova cópia de segurança.

Art. 13 A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas à COINF. A aprovação para execução da alteração depende da anuência do Gestor de Segurança da Informação.

Art. 14 Todo sistema/serviço desenvolvido ou internalizado pelo INPI deve ter sua estratégia de backup e periodicidade definida no momento que for entrar em produção. Parágrafo único. Estas definições devem constar no formulário de Demanda de Recursos de Infraestrutura da CGTI.

Art. 15 Todo sistema/serviço a ser descontinuado deverá ser submetido a um backup full e sua retenção deverá estar descrita no formulário de Requisição de Mudança na Infraestrutura em 4 Produção.

Art. 16 Os arquivos e documentos corporativos gerados pelos usuários e que necessitem integrar a rotina de backup deverão ser armazenados no servidor de arquivos, na rede interna corporativa. Parágrafo único. Os arquivos armazenados nas estações de trabalho não integram o escopo do processo de backup e não estarão disponíveis para recuperação, em caso de perda temporária ou definitiva do arquivo.

Art. 17 Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

Art. 18 A execução dos backups também deve ser orientada para que seus trabalhos respeitem as janelas (período de tempo) para execução, inclusive realizando previsão para a ampliação da capacidade dos dispositivos envolvidos no armazenamento.

Parágrafo único. Os procedimentos de backup serão realizados, diariamente, preferencialmente durante o período noturno, entre 22:00 (vinte e duas horas) e 06:00 (seis horas) do dia seguinte.

CAPÍTULO VI
DOS ARMAZENAMENTO E DESCARTE DAS MÍDIAS

Art. 19 As unidades de armazenamento utilizadas na salvaguarda 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. 20 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. 21 As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura e pressão, e com acesso restrito a pessoas autorizadas pela CGTI. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

Art. 22 Deverão ser adotados, sempre que possível e viável, controles criptográficos nos arquivos armazenados e nos arquivos que trafegam na rede do Instituto ou na Internet.

Art. 23 Além das cópias de segurança originais, deverão ser realizadas cópias de segurança com a finalidade de recuperação de desastres, que deverão ser armazenadas em local distante da origem dos dados.

§ 1º As cópias de segurança mensais e anuais poderão ser utilizadas como cópias de segurança com finalidade de recuperação de desastres, ficando a critério da CGTI decidir se manterá essas cópias armazenadas apenas em local distante dos dados originais ou também no local de backup original.

§ 2º Em virtude da constante evolução tecnológica, as cópias de segurança com finalidade de recuperação de desastres poderão ser armazenadas tanto em mídias tipo cartucho de fita quanto em outros formatos de armazenamento, de acordo com a solução de backup adotada pela CGTI.

§ 3º As cópias de segurança realizadas em mídias do tipo cartucho de fita e que tenham a finalidade de recuperação de desastres, deverão ser armazenadas no cofre de segurança do INPI, o mais distante possível da origem dos dados, observando-se a seguinte prioridade para ocupação da capacidade do cofre: 5 últimas anuais; 12 últimas mensais.

Art. 24 Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

CAPÍTULO VII
DO TESTE E PREVENÇAO DO PROCESSO DE RESTAURAÇÃO

Art. 25 Cabe aos administradores de backup, após prévia ciência e anuência do Gestor de Tecnologia da Informação do Instituto, a realização de testes periódicos de restauração, no intuito de averiguar os processos de backup e estabelecer melhorias.

§ 1º As políticas de backup devem ser testadas, ao menos, anualmente para garantir sua confiabilidade.

§ 2º Os testes de restore devem ser adequadamente documentados informando, minimamente, o tipo de ativo/sistema/serviço que teve o seu reestabelecimento testado, a data da

realização do teste de restore, o tempo gasto para o retorno do backup e se o restore foi concluído com sucesso.

CAPÍTULO VIII
DA RESTAURAÇÃO DE DADOS

Art. 26 As solicitações de restauração de sistemas/arquivos deverão ser abertas formalmente por meio de ferramenta de gestão de serviços de TI do Instituto. O atendimento deste dispositivo deverá obedecer às seguintes orientações:

I - A solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através de chamado técnico;

II - A restauração de objetos somente será possível nos casos em que estes tenham sido atingidos pela estratégia de backup;

III - O Gestor de Segurança da Informação terá a prerrogativa 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; e

IV - O tempo de restauração é proporcional ao volume de dados necessário para restore.

CAPÍTULO IX
DAS RESPONSABILIDADES

Art. 27 É de responsabilidade do Gestor de Segurança da Informação, em conjunto com o Comitê de Segurança da Informação, avaliar os estudos apresentados sobre tecnologias propostas na realização das cópias de segurança.

Art. 28 É de responsabilidade da Coordenação-Geral de Tecnologia da Informação - CGTI:

I - definir os procedimentos e orientações complementares necessários à aplicação das disposições estabelecidas nesta Portaria;

II - manter um plano de melhoria da infraestrutura de backup, e das rotinas de teste de restore;

III - definir os requisitos de backup e retenção definida para os equipamentos e serviços que estão sob gestão da CGTI; e

IV - gerenciar a realização de testes periódicos de restauração no intuito de averiguar a efetividade dos processos de backup e estabelecer melhorias.

Art. 29 É responsabilidade da Coordenação de Infraestrutura, Suporte e Segurança da Informação – COINF:

I - definir, juntamente com a área de negócios do INPI, os requisitos de backup e retenção estabelecido para o sistema ou serviço que está sendo desenvolvido ou implantado no INPI; e

II - acompanhar os testes de restore dos sistemas e serviços.

Art. 30 É responsabilidade das unidades gestoras dos sistemas/serviços do INPI:

I - informar sobre a necessidade de backup de sistema ou serviço que está sendo desenvolvido ou implantado no INPI que por ventura não esteja sob o escopo dos arquivos a serem armazenados;

II - definir o nível de sigilo necessário para os backups dos dados geridos por eles;

III - solicitar a restauração do backup, por meio da abertura de chamado específico, quando necessário;

IV - participar da elaboração dos Planos de Recuperação de Desastres e de Recuperação de Incidentes;

V - fornecer as informações sobre os requisitos legais de cada sistema ou serviço sob a sua gestão.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 31 Esta Portaria deve ser revisada e atualizada periodicamente, no máximo a cada 3 (três) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

Art. 32 Os casos omissos serão analisados pelo Comitê de Segurança da Informação.

Art. 33 Esta Portaria entra em vigor **01 de março de 2023**.

JULIO CESAR CASTELO BRANCO REIS MOREIRA
Diretor de Administração, no exercício da Presidência
Portaria de Pessoal MDIC nº 1, de 17/01/2023 - DOU de 18/01/2023

Documento assinado eletronicamente por **JULIO CESAR CASTELO BRANCO REIS MOREIRA**, **Presidente**, em 08/02/2023, às 10:59, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.inpi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0763299** e o código CRC **7E6B9275**.