TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO

# PORTARIA PRESI - 10264108

Institui a Política de *Backup* e Recuperação de Dados Digitais da Justiça Federal da 1ª Região.

O **PRESIDENTE DO TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO**, no uso de suas atribuições legais e regimentais e tendo em vista o constante nos autos do PAe 0014862-37.2018.4.01.8000,

**CONSIDERANDO:**

a) a Resolução CJF 6 de 7 de abril de 2008, que dispõe sobre a implantação da Política de Segurança da Informação e a utilização dos ativos de informática no âmbito do Conselho e da Justiça Federal de primeiro e segundo graus, tratando, entre outros assuntos, da elaboração de um Plano de Continuidade de Negócios como Documento Acessório Diferenciado;

b) a Instrução Normativa GSI/PR 1, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

c) as determinações do Tribunal de Contas da União contidas no Acórdão 2732/2017, item 9.6.1, para que se formule e se apresente ao TCU plano de ação para a criação de plano de continuidade de negócio e criação e implantação de política de geração de cópias de segurança dos dados cautelados pelo Tribunal (*backup* e restauração);

d) a Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização;

e) o *framework* Information Technology Infrastructure Library – ITIL, v. 3, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI;

f) o *framework* Control Objectives for Information and Related Technology – Cobit, v. 4, conjunto de boas práticas a serem aplicadas à governança da TI,

**RESOLVE:**

**Art. 1º** Instituir a Política de *Backup* e Recuperação de Dados Digitais da Justiça Federal da 1ª Região.

## CAPÍTULO I
## DAS DISPOSIÇÕES PRELIMINARES

**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 pelas unidades de tecnologia da informação (TI) e formalmente definidos como de necessária salvaguarda na Justiça Federal da 1ª Região.

**Art. 3º** A Política de que trata esta Portaria aplica-se a todas as unidades da 1ª Região que tenham sob sua guarda dados em suporte digital.

**Art. 4º** A salvaguarda e recuperação dos dados digitais da Justiça Federal da 1ª Região abrange exclusivamente repositórios institucionais custodiados pelas unidades de TI, armazenados nos centros de processamento de dados.

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.

**Art. 5º** A salvaguarda dos dados em formato digital pertencentes a serviços de TI da Justiça Federal da 1ª Região mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

## CAPÍTULO II
## DOS CONCEITOS E DEFINIÇÕES

**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;

II – área técnica: unidade responsável pela operação técnica dos ativos e serviços de TI;

III – ativo crítico: equipamento físico, unidade de armazenamento e dados que possuem elevada importância para a continuidade das atividades e serviços e concretização dos objetivos da organização;

IV – *backup*: cópia de segurança de dados computacionais, que pode ser utilizada ou consultada após sua restauração, em caso de indisponibilidade, perda ou alteração dos dados originais;

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 – *backup* 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 dados, documentos, unidades de armazenamento e acervos digitais;

X – disponibilidade: garantia de que o dado esteja acessível e utilizável sob demanda de pessoa física ou determinado serviço de TI, órgão ou entidade devidamente autorizados;

XI – gestor da informação: agente público formalmente responsável pela administração de serviço de TI e pelas informações produzidas em seu processo de trabalho;

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

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

XIV – operador de *backup*: pessoa responsável por procedimentos de atendimento de primeiro nível, acompanhamento de execução de rotinas de *backup*, realização de restaurações de arquivos de usuários, manutenção de troca de fitas no robô e gerenciamento de estoque de fitas locais;

XV – plano de continuidade de negócios (PCN): plano que define as etapas necessárias para recuperação dos processos de negócio logo após uma interrupção, identificando também os gatilhos para invocação, as pessoas a serem envolvidas, as comunicações, etc.

XVI – restauração: processo de recuperação e disponibilização de dados salvaguardados

em determinada imagem de *backup*;

XVII – retenção: período de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração;

XVIII – r*ecovery 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;

XIX – r*ecovery 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;

XX – rotina de *backup*: procedimento utilizado para se realizar um *backup*;

XXI – serviço de TI: sistema de informação ou qualquer solução de tecnologia da informação que armazene informações em formato digital;

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

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

## CAPÍTULO III
## DOS PADRÕES OPERACIONAIS

### Seção I
### Dos princípios gerais

**Art. 7º** A Política de *Backup* e Recuperação de Dados Digitais deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

**Art. 8º** As rotinas de *backup* devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

**Art. 9º** 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 críticos da organização.

**Art. 10.** Os serviços de TI críticos da Justiça Federal da 1ª Região devem ser formalmente elencados pelo Comitê de Gestão de Tecnologia da Informação da Justiça Federal da 1ª Região – CGTI-JF1.

Parágrafo único. Já ficam previamente estabelecidos os Processos, Judicial Eletrônico e Administrativo Eletrônico, como serviços críticos da Justiça Federal da 1ª Região.

### Seção II
### Das ferramentas de *backup*

**Art. 11.** As rotinas de *backup* devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

**Art. 12.** Os ativos envolvidos no processo de *backup* são considerados ativos críticos para a organização.

Parágrafo único. Compete à Secretaria de TI solicitar, à Administração, com as justificativas pertinentes, os equipamentos necessários para manter o parque de ativos sempre atualizado e em quantidade necessária ao atendimento da demanda da 1ª Região.

### Seção III
### Da frequência e retenção dos dados

**Art. 13.** Os *backups* dos serviços de TI críticos da Justiça Federal da 1ª Região devem ser realizados utilizando-se as seguintes frequências temporais:

I – diária;

II – semanal;

III – mensal;

IV – anual.

**Art. 14.** Os serviços de TI críticos da Justiça Federal da 1ª Região devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

I – diária: 2 meses;

II – semanal: 4 meses;

III – mensal: 1 ano;

IV – anual: 5 anos.

**Art. 15.** O *backup* de serviços de TI não críticos deve ser formalmente solicitado ao administrador de *backup* pelo responsável técnico pelo serviço de TI.

**Art. 16.** Os serviços de TI não críticos da Justiça Federal da 1ª Região devem ser resguardados observando-se o padrão mínimo de correlação frequência/retenção de dados estabelecida a seguir:

I – diária: 1 mês;

II – semanal: 2 meses;

III – mensal: 6 meses;

IV – anual: 2 anos.

**Art. 17.** Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.

**Art. 18.** A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pelos responsáveis técnicos dos serviços de TI, com a anuência prévia e formal dos gestores das informações, refletindo 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 deve explicitar, no mínimo, os seguintes requisitos técnicos:

I – escopo (dados digitais a serem salvaguardados);

II – tipo de *backup* (completo, incremental, diferencial);

III – frequência temporal de realização do *backup* (diária, semanal, mensal, anual);

IV – retenção;

V – RPO;

VI – RTO.

**Art. 19.** A recuperação de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança. Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de *backup*.

**Art. 20.** A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao administrador de *backup*. A aprovação para execução da alteração depende da anuência do gestor da informação e de prévia apreciação pelo CGTI-JF1.

Seção IV
Do uso da rede

**Art. 21.** O administrador de *backup* deve considerar o impacto da execução das rotinas de *backup* sobre o desempenho da rede de dados da Justiça Federal da 1ª Região, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da Justiça Federal da 1ª Região.

**Art. 22.** A execução do *backup* deve concentrar-se, preferencialmente, no período de

janela de *backup*.

**Art. 23.** O período de janela de *backup* deve ser determinado pelo administrador de *backup* em conjunto com a área técnica responsável pela administração da rede de dados da Justiça Federal da 1ª Região.

Seção V
Das unidades de armazenamento de *backups*

**Art. 24.** 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*;

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 pelos gestores das informações.

**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.** 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.

Seção VI
Dos testes de *backup*

**Art. 29.** Os *backups* devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

**Art. 30.** 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 em cada unidade da Justiça Federal da 1ª Região.

**Art. 31.** A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de *backup* serão definidos em norma específica a ser elaborada pela Secretaria de Tecnologia da Informação em conjunto com os gestores das informações.

## CAPÍTULO IV
## DAS RESPONSABILIDADES

**Art. 32.** O administrador de *backup* e o operador de *backup* devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de *backup*.

§ 1º O administrador e o operador de backup do TRF 1ª Região serão indicados pelo diretor da Secretaria de Tecnologia da |Informação (Secin), entre os servidores lotados na Seção de Equipamentos Corporativos (Seeco).

§ 2º Nas seções judiciárias, o administrador e o operador de backup serão indicados pelo diretor do Núcleo de Tecnologia da Informação (Nutec) ou pelo supervisor da Seção de Tecnologia da Informação (Seinf).

§ 3º Caso não seja possível, nas seccionais, a indicação de servidores distintos, o mesmo

servidor poderá exercer os papéis de administrador e operador de backup.

**Art. 33.** São atribuições do administrador de *backup*:

I – propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela Justiça Federal da 1ª Região;

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

III – configurar as soluções de *backup*;

IV – manter as unidades de armazenamento de *backups* preservadas, funcionais e seguras;

V – definir os procedimentos de restauração e neles auxiliar;

VI – verificar diariamente os eventos gerados pela solução de *backup*, tomando as providências necessárias para remediação de eventuais falhas;

VII – tomar medidas preventivas para evitar falhas;

VIII – reportar imediatamente ao setor a que está subordinado os incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de *backups*;

IX – gerenciar mensagens e registros de auditoria (LOGs) diários dos *backups*;

X – disponibilizar informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos *backups*;

XI – propor modificações visando ao aperfeiçoamento da Política de *Backup* e Recuperação de Dados Digitais, objeto desta Portaria;

XII – providenciar a execução dos testes de restauração.

**Art. 34.** São atribuições do operador de *backup*:

I – restaurar ou recuperar os *backups* em caso de necessidade;

II – operar e manusear as unidades de armazenamento de *backups*;

III – informar ao administrador de *backup* qualquer problema que impossibilite a restauração de um *backup*.

**Art. 35.** São atribuições das áreas técnicas:

I – solicitar restaurações de dados, com anuência do gestor da informação;

II – sanar dúvidas técnicas do administrador de *backup* acerca das informações salvaguardadas;

III – validar, tecnicamente, o resultado das restaurações eventualmente solicitadas;

IV – validar, tecnicamente, o resultado dos testes de restauração dos *backups*.

**Art. 36.** São atribuições dos gestores da informação:

I – solicitar, formalmente, a salvaguarda das informações geridas e dar anuência à solicitação feita pela área técnica para recuperação de dados;

II – validar, negocialmente, o resultado das restaurações eventualmente solicitadas;

III – validar, negocialmente, o resultado dos testes de restauração dos *backups.*

**Art. 37.** A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações.

Parágrafo único. O operador de *backup* 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.

## CAPÍTULO V

## DAS DISPOSIÇÕES FINAIS

**Art. 38.** Esta Portaria deverá ser amplamente divulgada no Tribunal e em todas as seções e subseções judiciárias da 1ª Região, fazendo-se ainda constar, em destaque, na área de tecnologia da informação na intranet do Tribunal, o *link* para sua publicação na biblioteca digital do Tribunal Regional Federal da 1ª Região.

**Art. 39.** Esta Portaria poderá ser revisada a qualquer tempo, para fins de eventual atualização, quando identificada a necessidade de alteração em qualquer de seus dispositivos.

**Art. 40.** A Secretaria de Tecnologia da Informação (no TRF 1ª Região), as unidades de TI (nas seções judiciárias) e os gestores das informações digitais tomarão as providências necessárias para a adequação das rotinas e dos procedimentos de *backups* definidos nesta Portaria.

Parágrafo único. Casos excepcionais não abordados nesta Portaria serão decididos pela Diretoria Geral, com análise da Secretaria de Tecnologia da Informação (no TRF 1ª Região), e sendo necessário, pelas unidades de TI (nas seções judiciárias) ou pelos gestores das informações digitais.

**Art. 41.** Esta Portaria em vigor na data de sua publicação.

Desembargador Federal **I'TALO FIORAVANTI SABO MENDES**

Presidente

Documento assinado eletronicamente por **I'talo Fioravanti Sabo Mendes**, **Presidente do TRF - 1ª Região**, em 10/06/2020, às 16:58 (horário de Brasília), conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://portal.trf1.jus.br/portaltrf1/servicos/verifica-processo.htm informando o código verificador **10264108** e o código CRC **57F01264**.