PORTARIA Nº CJF-POR-2018/00085 de 15 de março de 2018

Dispõe sobre a institucionalização da política de backup e restauração de arquivos do Conselho da Justiça Federal e dá outras providências

O SECRETÁRIO-GERAL DO CONSELHO DA JUSTIÇA FEDERAL, no uso de suas atribuições legais e tendo em vista o que consta no Processo n. CF-ADM-2012/00288, e

CONSIDERANDO a necessidade de atender às necessidades e expectativas do órgão quanto à redução de riscos e implementação com maior celeridade dos serviços de TI providos pela Secretaria de Tecnologia da Informação - STI;

CONSIDERANDO os termos da Resolução CNJ n. 211, de 15 de dezembro de 2015, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO os Acórdãos n. 1603/2008, 2308/2010, 2585/2012, 1200/2014 e 3051/2014, todos do Plenário do Tribunal de Contas da União, que recomendam a promoção de ações voltadas para a normatização e o aperfeiçoamento dos processos de governança, gestão e uso de tecnologia da informação e comunicação;

CONSIDERANDO as iniciativas constantes do caderno de estratégia do Conselho da Justiça Federal, estabelecidas pela Portaria n. CJF-POR-2015/00359, de 26 de agosto de 2015,

RESOLVE:

Art. 1º Institucionalizar a política de *backup* das informações eletrônicas no âmbito do Conselho da Justiça Federal - CJF, com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos dados sob a guarda da Secretaria de Tecnologia da Informação - STI, a fim de garantir a segurança, a integridade e a disponibilidade.

Art. 2º Para o disposto nesta portaria considera-se:

I - administrador de *backup*: é o responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de *backup* e *restore*;

II - administrador de recurso: é o responsável pela operação de determinados serviços ou equipamentos da STI;

III - *backup*: cópia de segurança de dados em meio digital;

IV - *backup* full: modalidade em que todos os dados são copiados integralmente;

V - *backup* incremental: modalidade em que somente os arquivos novos ou modificados são copiados;

VI - *backup* diferencial: modalidade em que os arquivos novos ou modificados da base de dados incremental são copiados;

VII - cliente de *backup*: é todo dispositivo ou equipamento onde é instalado o agente de *backup*;

VIII - *disaster recovery*: estratégia de recuperação de dados motivada por sinistros de grave amplitude, física ou lógica;

IX - mídia: meio físico no qual se armazenam os dados de *backup*;

X - retenção: período de tempo em que o conteúdo da mídia de *backup* deve ser preservado;

XI - *restore*: restauração de arquivos digitais;

XII - replicação de *backup*: segunda cópia de segurança realizada a partir da cópia original do *backup*, podendo ser armazenada em outro datacenter ou na nuvem.

Art. 3º A Subsecretaria de Infraestrutura e Suporte Técnico - SUTEC, da Secretaria de Tecnologia da Informação, será a unidade administradora do serviço de *backup*, ficando responsável pela política e procedimentos relativos aos serviços de *backup* e *restore*, bem como pela guarda das mídias, removíveis ou não, de acordo com as normas aplicáveis.

Art. 4º É atribuição do administrador de *backup*:

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

II - configurar a ferramenta de *backup*;

III - manter as mídias preservadas, funcionais e seguras;

IV - efetuar testes de *backup* e auxiliar nos procedimentos de *restore,* tanto no ambiente originário quanto no de replicação;

V - verificar diariamente os eventos gerados pela ferramenta de *backup*, tomando as providências necessárias para a remediação de falhas;

VI - restaurar os *backups* em caso de necessidade;

VII - gerenciar mensagens e logs diários dos *backups;*

VIII - comunicar ao administrador de recurso os erros e as ocorrências nos *backups*;

IX - propor modificações para o aperfeiçoamento da política de *backup*.

Parágrafo único. O serviço de *backup* deve ser orientado para a restauração das informações no menor tempo possível, principalmente havendo indisponibilidade de serviços que dependam da operação de *restore*.

Art. 5º É atribuição do administrador de recurso:

I - preencher documento de solicitação do serviço de *backup* e *restore* com as informações, tais como o servidor de rede e dados a serem incluídos;

II - dar permissão ao administrador de *backup* para configurar e modificar o agente de *backup* instalado no servidor de rede;

III - validar o resultado do *restore*.

Art. 6º A criação e a operação dos *backups* deverão obedecer às seguintes orientações:

I - criação de *backups*:

a) o *backup* deverá ser criado na ferramenta própria, seguindo as orientações do documento de solicitação do serviço, conforme requerido formalmente pelo administrador de recurso;

b) o *backup* deverá ser programado para a execução automática em horários de menor utilização dos sistemas e da rede de dados, conforme definição do administrador de *backup* em conjunto com o administrador de recurso.

II - operação de *backups*:

a) o *backup* deverá ser operado e monitorado pelo seu administrador;

b) para cada *backup* realizado com sucesso, deverá ser gerado um relatório automatizado pela própria ferramenta, confirmando a execução da operação;

c) para os *backups* que apresentarem falhas, o administrador de *backup* deverá criar relatório de acompanhamento, onde deverá constar a data, os horários de início e término, os objetos e os clientes de *backup*, a causa da falha, a ação corretiva adotada e qual parte do serviço restou comprometida.

Art. 7º A configuração e a monitoração das funcionalidades relativas às bases de dados dos *backups* serão de responsabilidade do administrador de recurso.

Art. 8º Os *backups* deverão seguir políticas diferenciadas de acordo com o tipo de dado e o ambiente computacional, conforme disposto a seguir:

I - quanto ao período de realização do *backup*:

a) diário: deverá ser programado para execução no intervalo entre 21h e 8h do dia seguinte, de segunda a sexta;

b) semanal: deverá ser programado para execução no intervalo entre 21h de sexta-feira e 8h da segunda-feira seguinte;

c) mensal: deverá ser programado para execução no primeiro fim de semana de cada mês entre 21h de sexta-feira e 8h da segunda-feira seguinte.

II - quanto à aplicação e retenção e replicação do *backup*:

a) ambiente de produção do CJF:

a1) proveniente de sistema de arquivos: diário, com retenção de 90 dias; semanal, com retenção de 26 semanas; e mensal, com retenção de 48 meses;

a2) proveniente de sistema operacional: diário, com retenção de 90 dias; semanal, com retenção de 26 semanas; e mensal, com retenção de 48 meses;

a3) proveniente de aplicação: diário, com retenção de 90 dias; semanal, com retenção de 26 semanas; e mensal, com retenção de 48 meses;

a4) proveniente de banco de dados: diário, com retenção de 90 dias; semanal, com retenção de 26 semanas; e mensal, com retenção de 48 meses.

b) ambiente de homologação e de desenvolvimento do CJF:

b1) proveniente de sistema de arquivos: diário, com retenção de 45 dias; e semanal, com retenção de 26 semanas;

b2) proveniente de sistema operacional: diário, com retenção de 45 dias; e semanal, com retenção de 26 semanas;

b3) proveniente de aplicação: diário, com retenção de 45 dias; e semanal, com retenção de 26 semanas;

b4) proveniente de banco de dados: diário, com retenção de 45 dias; e semanal, com retenção de 26 semanas.

c) ambiente de replicação:

c1) proveniente de sistema de arquivos: diário, com retenção de 90 dias; semanal, com retenção de 26 semanas; e mensal, com retenção de 12 meses;

c2) proveniente de sistema operacional: diário, com retenção de 90 dias; semanal, com retenção de 26 semanas; e mensal, com retenção de 12 meses;

c3) proveniente de aplicação: diário, com retenção de 90 dias; semanal, com retenção de 26 semanas; e mensal, com retenção de 12 meses;

c4) proveniente de banco de dados: diário, com retenção de 90 dias; semanal, com retenção de 26 semanas; e mensal, com retenção de 12 meses.

Parágrafo único. Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada ou destruída, conforme políticas de armazenamento de dados e de descarte vigentes.

Art. 9º Os *backups* de histórico de sistemas (log) e bancos de dados dos demais aplicativos do ambiente de produção da infraestrutura deverão seguir a mesma

política especificada para o *backup* do sistema de arquivos.

Art. 10. A recuperação de *backups* deverá obedecer às seguintes orientações:

I - o usuário que necessitar recuperar arquivos entrará em contato com o setor de suporte ao usuário, registrar o pedido no sistema de gestão de chamadas com, obrigatoriamente, as informações sobre o usuário, o arquivo a ser recuperado, o subdiretório de localização e a data da versão que deseja recuperar;

II - o chamado será encaminhado ao administrador de *backup*, que, após a conclusão da tarefa, realizará o fechamento do chamado indicando ao solicitante a restauração do arquivo;

III - deverá ser mantido registro de todos os arquivos restaurados juntamente com a solicitação inicial;

IV - os bancos de dados serão restaurados pelo administrador de recurso, devendo o administrador de *backup* auxiliá-lo na tarefa de *restore.*

Parágrafo único: Só será possível a restauração dos arquivos criados ou alterados no dia anterior ao da janela de realização do *backup*.

Art. 11. Os *backups* de produção com retenção mensal deverão ser testados periodicamente.

§ 1º Havendo detecção de falha ao efetuar o *backup* ou se este estiver incompleto, novo *backup* deverá ser executado com vistas ao seu armazenamento correto.

§ 2º Em caso de reincidência da execução descrita no § 1º deste artigo, o administrador de *backup* deverá registrar o incidente e submetê-lo à apreciação do administrador de recurso com vista à correção da aplicação do *backup*.

Art. 12. Quaisquer procedimentos programados nos equipamentos computacionais físicos ou virtuais que impliquem em riscos de funcionamento com interrupção dos sistemas e serviços essenciais do CJF somente deverão ser executados após a realização do *backup* dos seus dados.

Parágrafo único. Em casos excepcionais em que a urgência justifique, desde que autorizados pelo Secretário de Tecnologia da Informação, os procedimentos mencionados neste artigo poderão ser executados sem a realização de *backup*.

Art. 13. O descarte das mídias de *backup* inservíveis ou inutilizáveis deverá ser realizado mediante proposta apresentada pelo administrador de *backup* dirigida ao Secretário de Tecnologia da Informação.

Parágrafo único. As mídias a serem descartadas deverão ser destruídas de forma a impedir a sua reutilização ou acesso indevido às informações por pessoas não autorizadas.

Art. 14. Esta portaria entra em vigor na data de sua publicação.

Juiz Federal CLEBERSON JOSÉ ROCHA

PODER JUDICIÁRIO
JUSTIÇA FEDERAL
CONSELHO DA JUSTIÇA FEDERAL

DESPACHO Nº CJF-POR-2018/00085

Referência: CJF-POR-2018/00085 de 15 de março de 2018 - SECRETARIA-GERAL.
Assunto: Estudos e proposições para normas, regulamentações, diretrizes

Publicada no Boletim Interno Especial de 25/Junho/2018

Brasília, 26 de junho de 2018.

MARIA DAS GRAÇAS BARRETO DE MATOS
ASSISTENTE III
SEÇÃO DE PROTOCOLO E EXPEDIÇÃO

CJFPOR201800085B

Classif. documental	00.08.00.01