

PORTARIA Nº 623/ANVISA, DE 22 DE NOVEMBRO DE 2021

Institui a Política de Cópia de Segurança (Backup) e Restauração de Dados (Restore) da Anvisa.

O Diretor-Presidente da Agência Nacional de Vigilância Sanitária, no uso das atribuições que lhe confere o art. 47, inciso IX, aliado ao art. 54, III, § 3º do Regimento Interno aprovado pela Resolução de Diretoria Colegiada – RDC nº 255, de 10 de dezembro de 2018, **resolve**:

Art. 1º Fica instituída a Política de Cópia de Segurança (Backup) e Restauração de Dados (Restore) no âmbito da Agência Nacional de Vigilância Sanitária.

CAPÍTULO I DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para os fins desta Política, aplicam-se os seguintes conceitos e definições, além dos conceitos definidos no Glossário de Segurança da Informação, conforme Portaria nº 93, de 26 de setembro de 2019, do GSI/PR:

I - MÁQUINAS VIRTUAIS - arquivos de computador executados em um computador físico que se comportam como um computador físico;

II - GEOTI - Gerência de Operações em Tecnologia da Informação ou área responsável pela gestão da infraestrutura da TI;

III - GGTIN - Gerência-Geral da Tecnologia da Informação (TI) ou área responsável pela Tecnologia da Informação na Anvisa;

IV - GESIS - Gerência de Sistemas ou área responsável pela gestão dos sistemas e soluções de TI;

V - SERVIDOR - computador de alta capacidade que faz parte de uma rede corporativa, e que fornece serviços a outros computadores;

VI - SERVIDOR DE ARQUIVOS - servidor onde são armazenados os arquivos corporativos;

VII - BACKUP OU CÓPIA DE SEGURANÇA - conjunto de procedimentos que permitem salvaguardar os dados de um sistema 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;

VIII - RESTORE - restauração dos dados de um *backup*, quando existe a necessidade de recuperá-los.

CAPÍTULO II DA FINALIDADE

Art. 3º Esta política tem por finalidade:

I - estabelecer as diretrizes a serem seguidos para a realização de Cópias de Segurança e Restauração (*Backup e Restore*) no âmbito da Anvisa;

II - estabelece padrões para armazenagem, conservação e descarte de mídias de cópias de segurança, bem como padrões para a solicitação da restauração de arquivos;

III - atribuir papéis e responsabilidades aos envolvidos nas ações de cópias e restauração de dados.

Boletim de Serviço

Art. 4º A implantação desta política busca minimizar os impactos decorrentes da perda de dados, seja por falha humana ou por falha de equipamentos tecnológicos, bem como reduzir ao máximo o tempo de parada dos serviços de Tecnologia da Informação e Comunicação.

CAPÍTULO III DO ESCOPO

Art. 5º As orientações definidas neste documento devem ser implementadas por todos os setores da Anvisa que necessitem fazer cópias e restauração de informações em meio digital, que sejam mantidos em servidores pertencentes à Anvisa ou plataforma de nuvem adotada por esta Agência.

CAPÍTULO IV DOS BACKUPS, TIPOS E PERIODICIDADE

Art. 6º Os *backups* dos ativos de TI são classificados de acordo com a natureza dos dados conforme a seguir:

- I - Arquivos de Sistemas Operacionais;
- II - Arquivos de sistemas;
- III - Bancos de Dados;
- IV - Arquivos de logs;
- V - Servidor de E-mail;
- VI - Máquinas Virtuais;
- VII - Active Directory;
- VIII - Arquivos de configuração.

Art. 7º A definição da estratégia e da periodicidade do *backup* deve estar baseada no entendimento da aplicação, do seu ciclo de operação e dos seus volumes de dados (quantidade de informações).

Art. 8º Deverá ser adotada uma das estratégias a seguir para a classificação dos *backups*:

- I - Backup Completo (*full*): quando todos os dados são salvos;
- II - Backup Incremental/Cumulativo: quando os dados modificados ou criados entre o último *backup* (seja completo, diferencial ou incremental) são salvos;
- III - Backup Diferencial: quando somente os dados que mudaram ou foram criados depois do último *backup* completo são salvos.

Art. 9º A periodicidade e a retenção dos *backups* podem ser definidas em horas, dias, semanas, meses ou anos e deve estar relacionada ao tipo de mídia utilizada.

§ 1º A periodicidade e retenção mínimas dos *backups* serão definidos no ANEXO I desta Portaria e poderão ser alteradas a qualquer momento, conforme a necessidade da Anvisa, pela GGTIN.

§ 2º Os ativos de TI que, por motivos técnicos definidos pela GEOTI, não possam seguir por completo o padrão definido nesta Política, devem atender as diretrizes no que couber.

Art. 10. Todo sistema/serviço desenvolvido ou internalizado pela Anvisa deve ter sua estratégia de backup e periodicidade definida no momento que for entrar em produção.

Parágrafo único. Estas definições devem fazer parte da documentação dos sistemas/serviços.

Art. 11. Deverão ser realizados backups integrais (cópia/espelhamento da imagem dos servidores/máquinas envolvidos) periódicos de todos os sistemas/serviços críticos, de modo que, em caso de necessidade, tais sistemas/serviços possam ser recuperados em curtíssimo espaço de tempo.

Art. 12. 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 20:00 (vinte horas) e 06:00 (seis horas) do dia seguinte.

Art. 13. Todo sistema/serviço a ser descontinuado deverá ser submetido a um *backup full* e sua retenção deverá ser de, no mínimo, um ano.

Art. 14. Os arquivos e documentos corporativos gerados pelos usuários e que necessitem integrar a rotina de backup deverão ser armazenados no servidor de arquivos, na pasta corporativa da área que ficará armazenada no servidor ou na plataforma de nuvem contratada pela Anvisa.

§ 1º No caso de desligamento do usuário (de forma permanente ou temporária), o *backup* dos seus arquivos em nuvem deverão ser mantidos por, no mínimo, 90 (noventa) dias, após esse período os arquivos poderão ser excluídos a qualquer tempo.

§ 2º Cabe ao gestor da área do usuário desligado, solicitar por meio de abertura de um chamado, o *restore* os arquivos em nuvem de um usuário desligado da Anvisa na pasta corporativa da área.

§ 3º 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.

CAPÍTULO V DO ARMAZENAMENTO E DESCARTE DAS MÍDIAS

Art. 15. Todas as cópias de segurança devem ser guardadas em local seguro, bem como o seu acesso (físico e lógico) deve ser restrito a equipe técnica da GEOTI responsável por esse procedimento.

Art. 16. O local em que os *backups* são armazenados deve ser protegido contra agentes nocivos naturais (poeira, calor, umidade), bem como à prova de fogo.

Art. 17. O armazenamento dos backups poderá ser feito em fita, discos ou na plataforma de nuvem contratada pela Anvisa.

Art. 18. Deverá ser implementado controles criptográficos aos arquivos armazenados (*data at rest*), e aos arquivos que trafegam na rede da organização ou na Internet (*data in transit*).

Art. 19. Ao menos uma cópia dos arquivos de backup dos sistemas/serviços críticos deverá ser armazenada e mantida de modo off-line, isto é, não acessível pela rede da organização, seja

Boletim de Serviço

por meio de chamadas de sistema operacional, de chamadas de API (Application Programming Interface) ou por qualquer outro meio de acesso remoto.

Art. 20. As mídias devem ficar guardadas **preferencialmente** em cofre com segredo e chave.

§ 1º O segredo do cofre, quando houver, só será de conhecimento da equipe técnica da GEOTI.

§ 2º Uma cópia da chave deverá ficar em poder da pessoa que irá efetuar o *backup* e a outra no quadro de chaves da unidade organizacional responsável pelo procedimento de *backup*.

Art. 21. As mídias devem ser guardadas em condições de temperatura, umidade e pressão descritas pelo fabricante da mesma.

Art. 22. As mídias devem ser etiquetadas, contendo o código de identificação e outras informações relacionadas a esse ativo como data e hora do backup e tipo de backup efetuado.

Art. 23. As mídias a serem descartadas (devido à obsolescência tecnológica, ou defeito irreversível) devem ser eliminadas de forma segura e protegida, por meio de incineração, trituração, quebra, execução de procedimentos de sobrescrita de dados remanescentes (disco rígido) ou outro procedimento que impossibilite a recuperação dos dados por terceiros.

Art. 24. Deve ser feita o uso da tecnologia de espelhamento em tempo real dos servidores /serviços, sempre que possível, a fim de possibilitar um retorno mais rápido do sistema/serviço em caso de necessidade.

CAPÍTULO VI DO TESTE E PREVENÇÃO DO PROCESSO DE RESTAURAÇÃO

Art. 25. Cabe aos administradores de *backup*, em conjunto com os administradores de sistemas e infraestrutura, 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 Para sistemas/serviços críticos, os testes referentes as suas respectivas políticas de backup deverão ser realizadas quadrimestralmente.

§ 3º Os testes de *restore* devem ser adequadamente documentados informando, minimamente, o tipo de 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.

Art. 26. Deverá ser mantido um plano de amostragem simples, para a realização dos testes, conforme ANEXO II.

CAPÍTULO VIII DO SITE BACKUP

Art. 27. É desejável que se tenha um *site backup* em um local remoto ao da sede da Anvisa, que poderá ser utilizado, quanto necessário, para armazenar cópias extras dos principais backups e manter replicação de serviços de TI que são mantidos no Centro de Processamento de Dados, que se encontra na sede da Anvisa.

Boletim de Serviço

Parágrafo único. É obrigatória a anuência do Gerente-Geral da Tecnologia da Informação, antes de qualquer iniciativa para transmissão ou armazenamento de dados ou serviços para o site *backup*.

CAPÍTULO IX RESTAURAÇÃO DE DADOS (*RESTORE*)

Art. 28. As solicitações de restauração de sistemas/arquivos deverão ser abertas formalmente por meio de ferramenta de gestão de serviços de TI que deverá conter os nomes dos sistemas, arquivos e/ou pastas que deverão ser recuperados e, a data do arquivo que se pretende ter acesso, e se a restauração deverá sobrescrever o dado atual ou se será feita em um local diferente do original.

CAPÍTULO X DAS RESPONSABILIDADES

Art. 29. É de responsabilidade da Gerência de Operações em Tecnologia da Informação - GEOTI:

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 está sob gestão da GEOTI;

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

Art. 30. É responsabilidade da Gerência de Sistemas - GESIS:

I - definir, juntamente com a área de negócios da Anvisa, os requisitos de *backup* e retenção definida para o sistema ou serviço que está sendo desenvolvido ou implantado na Anvisa;

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

Art. 31. É responsabilidade das unidades gestoras dos sistemas/serviços da Anvisa.

I - informar sobre a necessidade de *backup* de sistema ou serviço que está sendo desenvolvido ou implantado na Anvisa que por ventura não esteja sob gestão da GGTIN;

II - definir, juntamente com a GESIS, os requisitos de *backup* e retenção para o sistema ou serviço que está sendo desenvolvido ou implantado na Anvisa segundo a legislação pertinente, quando houver previsão legal, e em alinhamento com as premissas institucionais ou requisitos de negócio;

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

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

V - definir a quantidade de informação que poderá ser perdida no caso de uma situação de desastre (RPO);

VI - definir o tempo máximo aceitável para a restauração de cópias de segurança dos sistemas de informação (RTO);

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

Boletim de Serviço

VIII - definir a tolerância ao tempo de *downtime* para a definição dos tipos e periodicidade das cópias de segurança, nos casos em que o procedimento de backup necessite ser executado com o sistema *offline*;

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

CAPÍTULO XI DAS DISPOSIÇÕES FINAIS

Art. 32. 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. 33. Os casos omissos serão analisados pelo Comitê Estratégico de Tecnologia da Informação - CETI.

Art. 34. Esta Portaria é de aplicação interna e entra em vigor na data de sua publicação no Boletim de Serviço.

ANTONIO BARRA TORRES

ANEXO I – RETENÇÃO E PERIODICIDADE DOS BACKUPS

Os planos de retenção e periodicidade dos backups devem seguir minimamente os requisitos abaixo.

Ativo de Backup: Bancos de Dados			
Ambiente	Estratégia de Backup	Retenção	Tipo de backup
Produção	Backup Completo: Semanal; Backup incremental: diário.	Backup Completo 20 (vinte) dias em disco e 6 meses em fita Backup incremental: 10 (dez) dias em disco	Estrutura lógica e dados
Homologação	Backup Completo: Semanal; Backup incremental: diário.	Backup Completo 10 (dez) dias em disco e 1 (um) mês em fita Backup incremental: 1 (uma) semana em disco.	Estrutura lógica e dados
Desenvolvimento	Backup Completo: Semanal.	Backup Completo: 10 (dez) dias em fita e 01 (um) mês em fita Backup incremental: 01 (uma) semana em disco	Estrutura lógica

Ativo de Backup: Servidores de Arquivos			
Ambiente	Estratégia de Backup	Retenção	Tipo de backup
Produção	Backup Completo: Semanal e Mensal Backup diferencial: diário	Backup Completo semanal: 2 (Duas) semanas em disco e 2 (Dois) meses em Fita. Backup Completo mensal: 2 (Duas) semanas em disco e 1 (Um) ano em fita. Backup diferencial: 1 (uma) semana em disco.	Sistema de arquivos

Ativo de Backup: Arquivos dos Sistemas Operacionais			
Ambiente	Estratégia de Backup	Retenção	Tipo de backup
Produção	Backup Completo: Semanal; Backup incremental: diário.	Backup Completo 3 (três) meses em disco; Backup incremental: 1 (um) mês em disco.	Sistema de arquivos

Boletim de Serviço

Ativo de Backup: Máquinas Virtuais

Ambiente	Estratégia de Backup	Retenção	Tipo de backup
Produção	Backup Completo: Semanal; Backup diferencial: diário.	Backup Completo 03 (três) meses em disco; Backup diferencial: 01 (uma) mês em disco.	Imagem das máquinas virtuais
Homologação	Backup Completo: Semanal; Backup diferencial: diário.	Backup Completo 03 (três) meses em disco; Backup diferencial: 01 (uma) mês em disco	Imagem das máquinas virtuais
Desenvolvimento	Backup Completo: Semanal; Backup diferencial: diário.	Backup Completo 1 (um) mês em disco; Backup diferencial: 01 (um) mês em disco	Imagem das máquinas virtuais

Ativo de Backup: Servidores de E-mail

Ambiente	Estratégia de Backup	Retenção	Tipo de backup
Produção	Backup Completo: Semanal e mensal Backup diferencial: diário.	Backup Completo 90 (Noventa) dias em disco e 6 Meses em Fita. Backup Completo 2 (Duas) semanas em disco e 2 (Anos) em fitas. Backup diferencial: 1 (um) mês.	Grupos de disponibilidade de bancos de dados

Ativo de Back: Descomissionamento de Máquina;

Ambiente	Estratégia de Backup	Retenção	Teste de Restore
Produção	Backup Completo	1 semana em disco e 5 anos em fita	Após a duplicação dos dados para a fita.
Homologação	Backup Completo	1 Semana em disco e 1 ano em fita	Após a duplicação dos dados para a fita.

Um plano detalhado dos *backups* efetuados deve ser produzido e disponibilizado na Wikitin no endereço: <http://doc.anvisa.gov.br/>

ANEXO II – PLANO DE AMOSTRAGEM

Os testes dos *backups* no ambiente computacional da Anvisa seguirão um Plano de amostragem simples, baseado na norma NBR 5427/1985, o qual consiste no padrão abaixo descrito:

Para cada Lote de **L** *backups* serão testados **A** amostra de uma mesma política de *backup* (ex: *backup* de banco de dados). Caso sejam encontrados até **X** *backups* com defeito, a amostra será aceita. Caso sejam encontrados **R** ou mais *backups* com defeito, a amostra será rejeitada. Vide quadro abaixo:

Lote (L)	Amostra (A)	Número de aceitação (X)	Número de rejeição (R)
500	10	1	2

Quando ocorrer de um lote ser rejeitado, a equipe da GEOTI da Anvisa acionará imediatamente um procedimento de revisão da política de *backup* rejeitada, bem como do ambiente a que se refere a mostra defeituosa.