PORTARIA MCOM Nº 4.547/2021 de 28 de janeiro de 2021

Aprova a Norma Complementar para Cópia de Segurança e Restauração de Dados .

A GESTORA DE SEGURANÇA DA INFORMAÇÃO, no uso das atribuições que lhe confere o inciso XII, do art. 2º, da Portaria nº 67/SEI-MCOM, de 4 de março de 2021, e tendo em vista o disposto no art. 15, inciso III, do Decreto nº 9.637, de 26 de dezembro de 2018, a Portaria MCOM Nº 2.454, de 22 de abril de 2021, os arts. 10, 15 e 19, da Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança institucional da Presidência da República, resolve:

Art. 1º Aprovar a Norma Complementar para Cópia de Segurança e Restauração de Dados.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

WANESSA QUEIROZ DE SOUZA OLIVEIRA
Gestora de Segurança da Informação

NORMA COMPLEMENTAR PARA CÓPIA DE SEGURANÇA E RESTAURAÇÃO DE DADOS

OBJETIVO
Esta norma tem por objetivo estabelecer a política de cópia de segurança e restauração de dados com as diretrizes para o processo de cópia e armazenamento dos dados sob a guarda da Coordenação-Geral de Tecnologia da Informação (CGTI), visando garantir a segurança, integridade e disponibilidade no âmbito do Ministério das Comunicações - MCOM.

APLICAÇÃO
Os termos definidos nesta norma aplicam-se a todos os agentes públicos do Ministério das Comunicações.

REFERÊNCIA LEGAL E NORMATIVA
Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
Instrução Normativa nº 2, de 24 de julho de 2020, altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
Portaria GSI/PR nº 93, de 18 de outubro de 2021, que aprova o glossário de segurança da informação;
Portaria MCOM Nº 2.454, de 22 de abril de 2021, que aprova a Política de Segurança da Informação do Ministério das Comunicações;
Portaria MCOM Nº 67, de 4 de março de 2021, que designa a Gestora de Segurança da Informação do

Ministério das Comunicações.
Acórdão nº 1109/2021 – TCU – Plenário, de 12 de maio de 2021.

1. CONCEITOS E DEFINIÇÕES:

1.1. Administrador de backup: agente público responsável pelos procedimentos de configuração, execução, monitoramento, elaboração de padrões, atendimentos avançados, resolução de incidentes, testes dos procedimentos de backup e restauração. O Coordenador de Infraestrutura e Serviços de Tecnologia da Informação deve ser designado com Administrador de Backup. O respectivo substituto deve ser designado entre os empregados ou servidores públicos da CGTI;

1.2. Gestor da informação: agente público formalmente responsável pela administração do serviço de TI e/ou sistema e pelas informações produzidas em seu processo de trabalho. Preferencialmente, deve ser um gestor da área negocial. O respectivo substituto deve ser, preferencialmente, da área negocial;

1.3. Ativo: tudo que tenha valor para a organização, material ou não (tais como informação, software, equipamentos, instalações, serviços, pessoas e imagem institucional);

1.4. Backup: 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;

1.5. Backup Completo (Full): modalidade de backup em que todos os dados a serem guardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último backup;

1.6. Backup Diferencial: modalidade de backup em que são guardados apenas dados novos ou modificados desde o último backup completo efetuado;

1.7. Backup Incremental: modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup - seja ele completo, diferencial ou incremental - são guardados;

1.8. Base de Dados ou Banco de Dados: coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;

1.9. Código fonte: é o conjunto de palavras ou símbolos escritos de forma ordenada, contendo instruções em uma das linguagens de programação existentes, de maneira lógica;

1.10. Criticidade: grau de importância da informação para a continuidade das atividades e serviços;

1.11. Custódia: consiste na responsabilidade de guardar um ativo para terceiros. A custódia não permite automaticamente o acesso ao ativo e nem o direito de conceder acesso a outros;

1.12. Dado: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;

1.13. Descarte: eliminação correta de informações, documentos, mídias e acervos digitais;

1.14. 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;

1.15. Incidente: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

1.16. Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

1.17. Janela de Backup: intervalo de tempo durante o qual as cópias de segurança sob execução agendada ou manual poderão ser executadas;

1.18. Log ou Registro de Auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional;

1.19. Mídia: mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação, inclui discos ópticos, magnéticos, compact disk (CD), fitas, papel, entre

outros. Um recurso multimídia combina sons, imagens e vídeos;

1.20. Nuvem: composta de rede de servidores remotos ao redor do globo que são conectados e operam como um único ecossistema. Estes servidores são responsáveis por armazenar e gerenciar dados, executar aplicativos ou fornecer serviços ou conteúdos, que podem ser acessados de qualquer dispositivo com acesso à Internet;

1.21. Plano de Backup: Documento formal onde são definidos os responsáveis pela cópia dos dados, o que será armazenado, periodicidade de execução da cópia e tempo de retenção, de acordo com as orientações da Política de Backup;

1.22. Repositório de Arquivo: Conjunto de documentos ou lugar onde os documentos são guardados;

1.23. Retenção: intervalo de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração; e

1.24. Rotina de Backup: procedimentos de realização de cópias de segurança.

2 DISPOSIÇÕES GERAIS

2.1. Esta Norma Complementar aplica-se a todos sistemas, bases de dados, máquinas físicas ou virtuais e repositórios de arquivos institucionais, em formato digital, em uso e de propriedade do Ministério das Comunicações.

2.2. Deverá ser elaborado um Plano de Backup, conforme requisitos presentes no item 3.1.3 desta Norma, para todos os sistemas, bases de dados, máquinas físicas ou virtuais e repositórios de arquivos institucionais do MCOM que serão objeto de cópias de segurança, 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.

2.3. Os dados armazenados localmente, em microcomputadores dos usuários ou em quaisquer outros dispositivos fora do centro de processamento de dados mantido pelo MCOM, ou que não façam parte de um plano de backup formalmente definido não terão backup e não haverá garantia de recuperação.

2.4. A guarda dos dados em formato digital pertencentes ao MCOM, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, devem estar garantidos nos acordos ou contratos que formalizam a relação entre os envolvidos.

2.5. São atribuições do administrador de backup:

a) propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pelo MCOM;

b) providenciar a criação e manutenção dos backups;

c) configurar as soluções de backup;

d) manter as unidades de armazenamento de backups preservadas, funcionais e seguras;

e) definir os procedimentos de restauração e neles auxiliar;

f) verificar os eventos gerados pela solução de backup, tomando as providências necessárias para remediação de eventuais falhas;

g) tomar medidas preventivas para evitar falhas;

h) gerenciar mensagens e registros de auditoria (LOGs) de execução dos backups;

i) disponibilizar informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos backups;

j) solicitar restaurações de dados, com anuência do gestor da informação;

k) propor modificações visando ao aperfeiçoamento desta Norma; e

l) providenciar a execução dos testes de restauração.

2.6. São atribuições dos gestores da informação:

a) solicitar, formalmente, a guarda das informações geridas;

b) solicitar, formalmente, a recuperação dos dados;

c) autorizar a solicitação de recuperação de dados feitas pela CGTI;

d) validar, negocialmente, o resultado das restaurações eventualmente solicitadas; e

e) validar, negocialmente, o resultado dos testes de restauração dos backups.

3 PROCEDIMENTOS

3.1. Solicitação de backup

3.1.1. As solicitações de backup devem ser realizadas pelo gestor da informação, em formulário

específico no Sistema de Processo Eletrônico, e enviadas ao administrador de backup.

3.1.2. O administrador de backup analisará a solicitação.

3.1.2.1. Não sendo viável o atendimento da solicitação, o administrador de backup encaminhará, pelo Sistema de Processo Eletrônico, resposta ao gestor da informação.

3.1.2.2. Sendo viável o atendimento, o administrador de backup deverá elaborar o Plano de Backup em conjunto com o gestor da informação, de modo a atender as necessidades específicas de negócio.

3.1.2.3. O administrador de backup, caso identifique a necessidade de guarda de informação, pode entrar em contato com o gestor da informação para a elaboração, em conjunto, do Plano de Backup.

3.1.3. O Plano de Backup, assinado pelo gestor da informação e pelo administrador do backup, deverá conter, no mínimo, as seguintes informações:

a) escopo: dados digitais a serem salvaguardados, com apontamento do local, tais como:

i) código fonte;

ii) banco de dados;

iii) repositório de arquivos;

iv) arquivos de configuração de servidores e ativos de rede; e

v) máquinas virtuais.

b) tipo de backup: completo, incremental, diferencial, podendo ser uma associação destes;

c) frequência temporal de realização do backup: diária, semanal, mensal, anual, podendo ser uma associação destes;

d) retenção: período em que o dado copiado no backup ficará retido e disponível para uso numa eventual recuperação antes de ser substituído por uma versão mais nova). Deverá ser definido com base na criticidade, frequência da atualização dos dados e características específicas de cada sistema;

e) unidade de armazenamento: indicação da unidade de armazenamento a ser utilizada, podendo ser storage, fita ou outras unidades em uso no MCOM.

f) local de armazenamento: indicação da localização de armazenamento do backup, incluindo se o backup é acessível por meio da rede, se não é acessível pela rede ou se a unidade de armazenamento se encontra em outra localidade remota, sendo em serviço de nuvem ou em edifício distinto do MCOM;

g) testes previstos: devem ser previstos a periodicidade, a abrangência e os procedimentos relativos aos testes que serão realizados;

h) procedimento de recuperação: documentar o procedimento para recuperar o backup quando necessário.

i) logs: previsão de criação e armazenamento de registros sobre a execução dos testes e das recuperações realizadas, a fim de detectar eventuais falhas e assegurar que houve a realização integral do backup.

j) RPO (recovery point objective): indicador que mensura o prazo máximo de perda dados em caso de incidentes; e

k) RTO (recovery time objective): indicador que mensura o tempo máximo em que um sistema ou uma informação pode ficar indisponível após um incidente.

3.1.4. Os backups devem ter, no mínimo, duas cópias realizadas em unidades de armazenamento distintos, sendo um online e outro offline ou disposto em outra localidade.

3.1.5. Os Planos de Backup devem ser criados e executados conforme os dispositivos desta Norma.

3.2. Rotinas de backup

3.2.1. As rotinas de backup devem ser realizadas em soluções específicas e próprias para esta finalidade, preferencialmente de forma automatizada.

3.2.2. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando um incidente ocasionar indisponibilidade de serviços de TI.

3.2.3. Os backups devem estar em conformidade com a legislação vigente, em especial ao que compete à LGPD.

3.2.4. Os backups, quando couber, devem ser criptografados, considerando as melhores práticas de mercado, normas vigentes e as ferramentas disponíveis.

3.2.5. Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.

3.2.6. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do MCOM, garantindo que o tráfego necessário às suas atividades não ocasione problemas aos demais serviços de TI.

3.2.7. A realização do backup deve ser, preferencialmente, concentrada no período de janela de backup,

definido pela CGTI.

3.2.8. 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.

3.3. Armazenamento de backup

3.3.1. Todos os ativos relacionados ao armazenamento dos backups devem ser acondicionados em locais apropriados, com controle de fatores ambientais sensíveis, como umidade e temperatura, e com acesso restrito a pessoas autorizadas pelo administrador de backup.

3.3.2. 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.

3.4. Testes de backup

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

3.4.2. Os testes de restauração dos backups devem ser realizados em equipamentos diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis.

3.4.3. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de backup devem ser devidamente registradas no plano de backup.

3.5. Restauração de backup

3.5.1. O gestor da informação deverá solicitar a restauração do backup, por meio do Sistema de Processo Eletrônico, indicando o que se deseja recuperar.

3.5.2. Caso o administrador de backup detecte a necessidade de restauração, deve entrar em contato com o gestor da informação e obter a anuência para a realização do procedimento.

3.5.3. Deverá ser mantido registro de todos os procedimentos adotados para a restauração do backup, juntamente com as informações do solicitante.

Documento assinado eletronicamente por **Wanessa Queiroz de Souza Oliveira**, **Gestora de Segurança da Informação**, em 28/01/2022, às 10:52 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site http://sei.mctic.gov.br/verifica.html, informando o código verificador **9296727** e o código CRC **405A5B99**.

Referência: Processo nº 53115.007158/2021-12 SEI nº 9296727