Instrução Normativa nº 03/2024

Institui Política de Backup e Recuperação de Dados Digitais da Nuvem Corporativa Estadual no âmbito da Administração Pública direta, autárquica e fundacional do Poder Executivo do Estado de Goiás.

O SECRETÁRIO-CHEFE DA SECRETARIA-GERAL DE GOVERNO, no uso das atribuições que lhe conferem os incisos I e II, § 1º do art. 40 da Constituição do Estado de Goiás; o inciso XIII do art. 5º e o caput c/c inciso I do § 2º do art. 108 da Lei estadual nº 21.792, de 16 de fevereiro de 2023; o inciso XIII do art. 2º, o inciso I do art. 75 e o inciso V do art. 81, do Decreto estadual nº 10.355, de 05 de dezembro de 2023,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Política de Backup e Recuperação de Dados Digitais da Nuvem Corporativa Estadual, nos termos desta Instrução Normativa, no âmbito da Administração Pública direta, autárquica e fundacional do Poder Executivo do Estado de Goiás.

Art. 2º Esta Instrução Normativa tem por objetivo criar diretrizes, requisitos básicos, responsabilidades e competências que visam à segurança, à proteção, à integridade e à disponibilidade dos dados digitais sob custódia da Unidade Central de Tecnologia da Informação, para se manter a continuidade do negócio.

Art. 3º A salvaguarda e recuperação dos dados digitais abrange exclusivamente dados armazenados na infraestrutura de tecnologia da informação da Nuvem Corporativa Estadual, mantida e gerida pela Unidade Central de Tecnologia da Informação.

Parágrafo único. Não serão salvaguardados nem recuperados dados armazenados localmente nos microcomputadores dos usuários ou em quaisquer outros sistemas que porventura estiverem hospedados fora da Nuvem Corporativa Estadual, ficando sob a responsabilidade do usuário a cópia de seus dados locais para os servidores de armazenamento de arquivos.

Art. 4º A salvaguarda dos dados em formato digital pertencentes a serviços de computação em nuvem disponibilizados pela Unidade Central de Tecnologia da Informação, mas hospedados em ambiente de nuvem pública, seguirá as políticas e definições acordadas nos contratos de prestação de serviço que formalizem a relação entre os envolvidos, e serão informadas em Plano de Backup específico.

Art. 5º A Unidade Central de Tecnologia da Informação se reserva ao direito de realizar, a qualquer momento, a exclusão de recursos ou dados digitais das rotinas de backup, ou alteração nos tempos de retenção, mediante justa necessidade técnica, que deve ser previamente informada ao Proprietário da Informação, e atualizada no Plano de Backup relacionado.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 6º Para os fins desta Instrução Normativa, considera-se:

I - administrador de backup: unidade administrativa integrante da Unidade Central de Tecnologia da Informação, responsável pelo planejamento de soluções de backup, definição de padrões, configurações e atendimento avançado de resolução de incidentes e problemas referentes a backups;

II - backup ou cópia de segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação em caso de perda ou alteração dos dados originais;

III - backup completo: estratégia de backup que promove a cópia de segurança completa de todos os dados de um sistema computacional para um repositório de dados, independentemente de terem sido ou não alterados desde o último backup;

IV - backup diferencial: estratégia de backup que promove a cópia de segurança somente dos dados novos ou modificados de um sistema computacional desde o último backup completo;

V - backup incremental: estratégia de backup que promove a cópia de segurança somente dos dados novos ou modificados de um sistema computacional desde o último backup, independente da modalidade;

VI - backup on-site: cópia de segurança que, uma vez realizada, é acessível dentro do mesmo Data Center;

VII - backup off-site: cópia de segurança que, uma vez realizada, é armazenada em outro Data Center geograficamente separado ou em serviço de backup em nuvem;

VIII - custódia: consiste na responsabilidade de guardar um ativo para terceiros, sem permitir acesso automático ou o direito de conceder acesso a outros;

IX - 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;

X - janela de backup: período durante o qual cópias de segurança sob execução agendada poderão ser executadas;

XI - integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XII - Nuvem Corporativa Estadual: infraestrutura tecnológica capaz de suportar demandas de hospedagem de serviços de computação em nuvem, processados e armazenados nos Data Centers estaduais e em ambiente de nuvem pública e privada, sob gestão e operacionalização da Unidade Central de Tecnologia da Informação;

XIII - plano de backup: planejamento que detalha a execução da Política de Backup, no qual são informados os requisitos e as rotinas/roteiros de backup de cada conjunto de dados ou informação a serem salvaguardados;

XIV - proprietário da informação: área interessada do órgão ou indivíduo legalmente instituído por sua posição ou cargo, que é responsável primário pela viabilidade e sobrevivência da informação, e que pode requisitar a restauração dos dados digitais por ele gerenciados;

XV - *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;

XVI - *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;

XVII - repositório de dados de backup: unidade de armazenamento com características específicas para retenção de cópia de segurança de dados digitais;

XVIII - restauração: processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de backup;

XIX - retenção: período pelo qual os dados devem ser salvaguardados e estarem aptos à restauração;

XX - rotina/roteiro de backup: conjunto de procedimentos utilizados para se realizar um backup;

XXI - snapshot: ponto de restauração de máquinas virtuais que permite o retorno a um estado anterior;

XXII - Unidade Central de Tecnologia da Informação: unidade central que coordena a gestão de Tecnologia da Informação no âmbito do Estado de Goiás, atualmente, a Subsecretaria de Tecnologia da Informação, da Secretaria-Geral de Governo, com suas respectivas unidades básicas e complementares; e

XXIII - Unidades Setoriais de Tecnologia da Informação: unidade administrativa, pertencente a órgão ou entidade estadual, responsável por atuar nas atividades de Tecnologia da Informação, sob o direcionamento técnico da Unidade Central de Tecnologia da Informação.

CAPÍTULO III

DAS DIRETRIZES

Art. 7º São diretrizes da Política de Backup e Recuperação de Dados Digitais da Nuvem Corporativa Estadual:

I - assegurar o acesso contínuo às informações definidas por esta Instrução Normativa, por meio de procedimentos para backup e restauração que observem criteriosamente o modo e a periodicidade de cada cópia de segurança dos dados;

II - garantir que todos os sistemas de informação críticos façam parte da rotina de backup, para um restabelecimento completo e no menor tempo possível, assegurando a continuidade do negócio em caso de desastres;

III - prover resiliência dos dados por meio do armazenamento de diversas cópias de backup dos dados originais, espalhadas por repositórios de dados diferentes e replicadas, e armazenadas remotamente em localidade geograficamente distante e segura;

IV - certificar que as rotinas de backup possuam requisitos mínimos diferenciados de acordo com o tipo de serviço, recurso ou dado salvaguardado, dando prioridade aos serviços ou recursos definidos como críticos pelos proprietários da informação;

V - atestar que as rotinas de backup utilizem soluções próprias e especializadas para este fim, de forma que as tarefas de backup sejam realizadas de forma automatizada, assim como as rotinas de testes de integridade e recuperabilidade; e

VI - resguardar que as rotinas de backup atendam aos requisitos mínimos de segurança da informação e demais requisitos legais e normativos, especialmente os relacionados à Lei Geral de Proteção de Dados Pessoais - LGPD, Lei federal nº 13.709, de 14 de agosto de 2018, e à norma ABNT NBR ISO/IEC 27002:2013.

CAPÍTULO IV

DAS FERRAMENTAS DE BACKUP

Art. 8º As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, que possuam funcionalidades de automatização das rotinas, e de realização de testes de integridade e recuperabilidade dos dados digitais protegidos.

Art. 9º Os equipamentos, softwares e demais componentes envolvidos no processo de backup são considerados ativos críticos para a Unidade Central de Tecnologia de Informação.

CAPÍTULO V

DA FREQUÊNCIA E RETENÇÃO DOS DADOS

Art. 10. As rotinas de backup do ambiente da Nuvem Corporativa Estadual devem ser realizadas com a frequência diária, incluindo finais de semana e feriados.

Parágrafo único. Deverá ser avaliado pelo proprietário da informação, em conjunto com o administrador de backup, a necessidade de realização de cópias de segurança dos dados digitais em frequência menor que a diária, conforme a criticidade do serviço ou recurso.

Art. 11. Os serviços e recursos hospedados na Nuvem Corporativa Estadual devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/tempo de retenção de dados/RPO e RTO estabelecida a seguir:

I - Frequência: Diária;

II - Tempo de Retenção de Dados: 4 (quatro) semanas;

III - *Recovery Point Objective* (RPO): 24 (vinte e quatro) horas; e

IV - *Recovery Time Objective* (RTO): 4 (quatro) horas.

Art. 12. Poderão ser estabelecidos frequência, tempo de retenção, RPO e RTO diferenciados para cada sistema de informação ou dados digitais, de acordo com o nível de criticidade, mediante solicitação formal e justificativa motivada do proprietário da informação.

Art. 13. Poderão ser realizados, mediante solicitação e justificativa formal, backups extras individualizados, de forma a atender demandas específicas e excepcionais, à exemplo de necessidades legais ou de litígio de maior tempo de retenção, mudanças e manutenções no ambiente, ou desativação de servidores virtuais que requeiram um tempo maior de retenção dos dados digitais para possíveis auditorias futuras.

Art. 14. A recuperação de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança.

Art. 15. Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de backup.

Art. 16. Na ocorrência de falha ou incompletude de alguma rotina de backup, uma nova rotina deve ser executada visando ao armazenamento, sendo que o administrador de backup deve identificar a causa da falha e adotar ação corretiva antes da execução da próxima rotina agendada.

Art. 17. O *Recovery Time Objective* (RTO) desta Instrução Normativa refere-se a incidentes ou falhas que não afetam de maneira significativa o ambiente computacional, não se aplicando a situações de desastres causados por eventos incontroláveis, classificados como força maior ou caso fortuito, que afetem todo ou grande parte do ambiente.

CAPÍTULO VI

DO PLANO DE BACKUP

Art. 18. O plano de backup deve conter as rotinas de backup para cada grupo de serviço ou recurso que armazene dados digitais, cumprindo as diretrizes desta Política, refletindo os requisitos de negócio do órgão ou entidade, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

I - escopo do plano de backup: definir quais os dados digitais a serem salvaguardados e quaisquer exceções ao escopo definido;

II - tipo do backup: definir a estratégia da cópia dos dados digitais, como completo, incremental ou diferencial;

III - frequência de realização: definir a periodicidade como diária, semanal, mensal ou anual;

IV - tempo de retenção: definir o tempo de acordo com o nível de criticidade ou requisitos legais;

V - janela de backup: definir o período preferencial para a execução das cópias de segurança;

VI - RPO: definir o prazo máximo aceitável de perda de dados em caso de incidente;

VII - RTO: definir o prazo máximo aceitável de inoperância dos serviços de TI até a restauração dos dados após um incidente;

VIII - repositório de dados de backup: informar as unidades de armazenamento e locais seguros, diferentes do local original, e a replicação dos dados;

IX - estratégia de backup: informar as tecnologias e soluções que serão utilizadas na execução das cópias de segurança, e como se dará o monitoramento dos resultados das rotinas;

X - procedimentos de teste de integridade: detalhar os procedimentos de teste de recuperação das cópias de segurança para detectar tempestivamente eventuais falhas lógicas e físicas;

XI - periodicidade do teste de integridade: informar o período regular de teste de restauração das cópias de segurança, conforme definido nesta Política;

XII - procedimento de restauração: detalhar os procedimentos para realizar a restauração das cópias de segurança, quando necessário;

XIII - requisitos de segurança da informação: definir os controles de acesso lógico, uso de criptografia, imutabilidade, entre outros;

XIV - requisitos legais e normativos: informar, caso aplicável, as legislações, regulamentações de conformidade ou de litígio que determinam tempo de retenção diferenciado para os dados salvaguardados ou determinada frequência de backup; e

XV - aprovação: aprovação e assinatura dos responsáveis pela execução e gestão das rotinas de backup, bem como das demais partes interessadas.

Art. 19. Os planos de backup devem ser aprovados pelo administrador de backup, comunicados às partes interessadas (Unidades Setoriais de TI e proprietários das informações) e devidamente publicados e disponibilizados.

CAPÍTULO VII

DA JANELA DE EXECUÇÃO DAS ROTINAS DE BACKUP

Art. 20. A execução das rotinas de backup deve ser concentrada, preferencialmente, no período definido como janela de backup.

Parágrafo único. Para definição da janela de backup, deve-se considerar o impacto das rotinas de backup no desempenho da rede computacional, garantindo que o tráfego necessário não cause indisponibilidade dos recursos computacionais e sistemas durante o horário de expediente.

Art. 21. O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com o proprietário da informação.

CAPÍTULO VIII

DOS REPOSITÓRIOS DE DADOS DE BACKUP

Art. 22. As unidades de armazenamento utilizadas como repositórios de dados de backup devem considerar as seguintes características dos dados resguardados:

I - criticidade dos dados salvaguardados;

II - requisitos de segurança da informação;

III - tempo de retenção dos dados;

IV - probabilidade de necessidade de restauração;

V - tempo esperado para restauração;

VI - custo de aquisição das unidades de armazenamento de backup; e

VII - vida útil da unidade de armazenamento de backup.

Art. 23. 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. 24. A execução das rotinas de backup deve prever a ampliação da capacidade dos dispositivos envolvidos no armazenamento.

Art. 25. O administrador de backup deve avaliar 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 e deduplicação de dados, desde que o acréscimo no tempo de backup e de recuperação dos dados seja considerado aceitável.

Art. 27. Os backups devem ter, no mínimo, 2 (duas) cópias realizadas em repositórios de dados distintos, sendo uma on-site e outra off-site.

Art. 28. Os backups que contenham dados sensíveis e que requeiram tratamento específico quanto à segurança da informação devem ser criptografados e ter seus acessos devidamente controlados.

Art. 29. Os repositórios de backup devem possuir funcionalidade de imutabilidade, fornecendo proteção adicional contra possíveis ataques de *ransomware*.

Art. 30. Os repositórios de backup devem ser fisicamente separados do ambiente dos dados digitais de produção, sendo utilizados exclusivamente para a salvaguarda dos dados digitais, sem compartilhamento de recursos para outras finalidades.

Art. 31. A vida útil das unidades de armazenamento que compõem os repositórios de backup deve ser de, no mínimo, 5 (cinco) anos.

Art. 32. Quando houver necessidade de descarte de unidades de armazenamento de backups, estas devem ser logicamente destruídas para garantir a inutilização e sanitização dos dados, observando-se práticas de descarte sustentável e ambientalmente corretas.

CAPÍTULO IX

DOS TESTES DE INTEGRIDADE DE BACKUP

Art. 33. Os backups devem ser testados periodicamente para garantir sua confiabilidade e a integridade dos dados salvaguardados.

Art. 34. O administrador de backup deve elaborar um cronograma de testes, priorizando os backups mais importantes para a continuidade das rotinas de trabalho, conforme o nível de criticidade ou relevância dos dados, aplicações e sistemas, com o conhecimento e concordância do proprietário da informação.

§ 1º Após uma restauração bem-sucedida, o proprietário da informação deve realizar os testes de validação da integridade dos dados.

§ 2º O teste de integridade será considerado válido quando o ambiente original puder ser recriado em um estado consistente.

§ 3º Ações corretivas devem ser tomadas sempre que problemas de backup forem identificados durante os testes de integridade, visando reduzir os riscos associados a backups falhos.

§ 4º Os resultados dos testes de integridade devem ser devidamente documentados.

Art. 35. Os testes de restauração e integridade dos backups de dados digitais categorizados como críticos devem ser realizados quadrimestralmente, enquanto os de dados não críticos devem ser realizados, no mínimo, anualmente.

Art. 36. Os testes de restauração e integridade dos backups devem ser realizados por amostragem, em equipamentos servidores diferentes dos que atendem os ambientes de produção, considerando os recursos humanos e tecnológicos disponíveis.

Parágrafo único. Sempre que possível, os testes de restauração e integridade dos backups devem ser realizados de forma automática, simulando um ambiente produtivo e realizando as devidas validações customizadas pelo proprietário da informação.

Art. 37. A periodicidade, a abrangência, os procedimentos e as rotinas dos testes de integridade serão definidos no plano de backup.

CAPÍTULO X

DAS RESPONSABILIDADES

Art. 38. São atribuições da Unidade Central de Tecnologia da Informação, por intermédio dos administradores de backup:

I - garantir a disponibilização de infraestrutura e recursos adequados para a realização dos procedimentos de backup;

II - apresentar soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela Unidade Central de Tecnologia da Informação;

III - propor modificações visando o aperfeiçoamento desta Política de Backup e Recuperação de Dados Digitais da Nuvem Corporativa Estadual;

IV - elaborar os planos de backup específicos para cada grupo de serviço ou recurso que armazene dados digitais;

V - providenciar a criação e manutenção das rotinas de backup;

VI - gerir e manter os componentes e ferramentas envolvidas nas rotinas de backup;

VII - preservar, manter funcionais e garantir a segurança dos repositórios de dados de backup;

VIII - realizar a execução dos testes de integridade e restauração;

IX - providenciar a recuperação dos backups em caso de necessidade;

X - implementar e manter procedimentos de controle de acesso e segurança da informação para garantir ao máximo o não vazamento das informações;

XI - tratar e zelar pela segurança dos dados salvaguardados, de acordo com os princípios e diretrizes da Lei Geral de Proteção de Dados Pessoais - LGPD;

XII - disponibilizar informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos backups;

XIII - providenciar a verificação diária dos eventos gerados pela solução de backup, tomando as providências necessárias para remediar eventuais falhas;

XIV - sanar dúvidas técnicas do proprietário da informação e das Unidades Setoriais de Tecnologia da Informação acerca das informações salvaguardadas;

XV - manter profissionais com alto grau de conhecimento sobre as ferramentas e componentes da solução de backup, com capacidade de realizar ajustes finos no ambiente conforme as melhores práticas de mercado; e

XVI - promover medidas preventivas para evitar falhas nas rotinas de backup.

Art. 39. São atribuições dos proprietários da informação:

I - informar, mediante justificativa formal e motivada, quais serviços e dados necessitam de rotina de backup diferente do padrão estabelecido nesta Instrução Normativa, especificando o escopo de dados, a frequência e o tempo de retenção apropriados, e demais informações relevantes; e

II - providenciar a validação, negocialmente, do resultado das restaurações solicitadas e dos testes de restauração dos backups dos dados sob sua responsabilidade.

Art. 40. São atribuições das Unidades Setoriais de Tecnologia da Informação:

I - analisar e encaminhar à Unidade Central de Tecnologia da Informação as solicitações e justificativas dos proprietários da informação referentes às necessidades de rotinas de backup e restaurações;

II - garantir que quaisquer procedimentos programados nos servidores virtuais sob sua responsabilidade, que impliquem em riscos de funcionamento ou perda de informação, sejam executados somente após a realização de snapshot ou backup desses servidores;

III - assegurar que, no âmbito de seu órgão ou entidade, os usuários armazenem os documentos institucionais nos servidores de armazenamento da Nuvem Corporativa Estadual; e

IV - submeter previamente à Unidade Central de Tecnologia da Informação quaisquer alterações, projetos ou demandas que necessitem de grande quantidade de recursos de armazenamento e possam afetar os procedimentos de backup, a fim de possibilitar o planejamento adequado de capacidade da infraestrutura necessária.

CAPÍTULO XI

DAS DISPOSIÇÕES FINAIS

Art. 41. Compete à Unidade Central de Tecnologia da Informação a revisão, atualização e divulgação desta Instrução Normativa sempre que necessário.

Art. 42. A Unidade Central de Tecnologia da Informação, as Unidades Setoriais de Tecnologia da Informação e os proprietários das informações terão o prazo de 180 (cento e oitenta) dias

para adequarem as rotinas e procedimentos de backup às diretrizes definidas nesta Instrução Normativa.

Art. 43. Os casos omissos serão dirimidos pela Unidade Central de Tecnologia da Informação, por intermédio de suas unidades administrativas.

Art. 44. Esta Instrução Normativa entra em vigor na data de sua publicação.

Gabinete do Secretário-Chefe da Secretaria-Geral de Governo, aos dias de de 2024.

ADRIANO DA ROCHA LIMA
Secretário-Chefe da Secretaria-Geral de Governo

Documento assinado eletronicamente por **ADRIANO DA ROCHA LIMA**, **Secretário (a)**, em 28/08/2024, às 18:45, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

A autenticidade do documento pode ser conferida no site **http://sei.go.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=1** informando o código verificador **63585087** e o código CRC **A205A30D**.