Boletim de Serviço Eletrônico em 31/07/2024
DOU de 31/07/2024, seção 1, página 107 e 108

FUNDAÇÃO ALEXANDRE DE GUSMÃO

PORTARIA FUNAG Nº 85, DE 30 DE JULHO DE 2024

Institui a Política de Backup e Restauração de Dados Digitais no âmbito da Fundação Alexandre de Gusmão

O PRESIDENTE, SUBSTITUTO, DA FUNDAÇÃO ALEXANDRE DE GUSMÃO - FUNAG, no exercício das atribuições previstas no inciso V do art. 15 do anexo I do Decreto nº 10.943, de 24 de janeiro de 2022, e § 1º do art. 17 da Portaria FUNAG nº 65, de 8 de fevereiro de 2022, e tendo em vista o disposto no art. 15, inciso I, Decreto nº 9.637, de 26 de dezembro de 2018, na Lei nº 13.709, de 14 agosto de 2018, na Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 e na Portaria SGD/MGI nº 852, de 28 de março de 2023, resolve:

Art. 1º Aprovar a Política de **Backup** e Restauração de Dados Digitais da Fundação Alexandre de Gusmão, na forma do Anexo desta portaria.

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

DIRCEU RICARDO LEMOS CECCATTO

Documento assinado eletronicamente por **Dirceu Ricardo Lemos Ceccatto**, **Presidente, substituto**, em 30/07/2024, às 15:39, conforme horário oficial de Brasília, com fundamento no § 2º 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.funag.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0090177** e o código CRC **FF5F5E6B**.

ANEXO

POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS DIGITAIS

CAPÍTULO I

ESCOPO E ABRANGÊNCIA

Art. 1º A Política de **Backup** e Restauração de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pela Divisão de Tecnologia da Informação e formalmente definidos como de necessária salvaguarda na Fundação Alexandre de Gusmão, para se manter a continuidade do negócio.

Art. 2º Esta política se aplica a todos os dados no âmbito da Fundação, incluindo dados armazenados em serviços de nuvem Pública ou Privada.

§1º Esta política se aplica a todos os servidores, estagiários e colaboradores que, direta ou indiretamente, podem ser criadores e/ou usuários de dados da Fundação, bem como a terceiros que acessam e usam sistemas e equipamentos de tecnologia da informação ou que criam, processam ou armazenam dados de propriedade da FUNAG.

§2º 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 pela Divisão de Tecnologia da Informação, ficando sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s).

§3º A salvaguarda dos dados em formato digital pertencentes a serviços de tecnologia da informação da FUNAG 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

CONCEITOS E DEFINIÇÕES

Art. 3º Para os fins desta Política, considera-se:

I - administrador de **backup:** agente responsável pela gestão dos procedimentos de **backup** incluindo a definição de padrões referentes a configuração, execução, monitoramento e testes de **backups** e restauração de dados;

II - área técnica: unidade responsável pela operação técnica e execução dos procedimentos de **backup** e restauração de dados;

III - gestor da informação: qualquer indivíduo ou estrutura de órgão ou entidade da Administração Pública Federal, direta e indireta, que tenha responsabilidade formal pela operação do serviço ou sistema de Tecnologia da Informação (TI) e pelas informações produzidas em seu processo de trabalho;

IV - **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;

V - dados críticos: são dados considerados críticos para o funcionamento da instituição, cuja perda acarreta na interrupção de serviços essenciais e danos à reputação da entidade;

VI - eliminação: exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

VII - mídia: mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação - inclui discos ópticos, magnéticos, CDs, fitas e papel, entre outros.

Um recurso multimídia combina sons, imagens e vídeos;

VIII - infraestrutura crítica: instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança;

IX - **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; e

X - **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.

CAPÍTULO III

DOS PADRÕES OPERACIONAIS

Seção I

Dos princípios gerais

Art. 4º A Política de **Backup** e Restauração de Dados deve estar alinhada com à Política de Segurança da Informação da FUNAG.

Art. 5º A Política de **Backup** e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

Art. 6º 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. 7º As rotinas de **backup** devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

Art. 8º 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. 9º O armazenamento de **backup**, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um sítio de **backup** em um local remoto ao da sede da organização para armazenar cópias extras dos principais **backups**, a exemplo dos **backups** de dados de serviços críticos.

Art. 10. A infraestrutura de rede de **backup** deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.

Art. 11. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de **backup.**

Art. 12. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Seção II

Da frequência e retenção dos dados

Art. 13. Os **backups** dos serviços de TI críticos da FUNAG devem ser realizados utilizando-se as seguintes frequências temporais:

I - diário;

II - semanal;

III - mensal; e

IV – anual.

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

I - diária: 30 dias;

II - semanal: 4 semanas;

III - mensal: 4 meses; e

IV - anual: 2 anos.

Art. 15. Os serviços de TI não críticos da FUNAG devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

I - diária: 15 dias;

II - semanal: 2 semanas;

III - mensal: 2 meses; e

IV - anual: 1 ano.

Art. 16. Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.

Art. 17. Os ativos envolvidos no processo de **backup** são considerados ativos críticos para a organização.

Art. 18. A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pelo gestor da informação, com a anuência prévia e formal do administrador de **backup**, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação e proteção de dados 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; e

VI - RTO.

Art. 19. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao administrador de **backup** e a aprovação para execução da alteração depende da anuência do gestor da informação.

Art. 20. Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de **backup** deverão zelar pelo cumprimento das diretrizes estabelecidas.

Seção III

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 FUNAG, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI.

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 FUNAG.

Seção IV

Do armazenamento

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**; e

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 restauração dos dados seja considerado aceitável pelos gestores das informações.

Art. 27. A execução das rotinas de **backup** deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

Art. 28. As unidades de armazenamento de backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas pelo administrador de **backup**. Além disso as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

Art. 29. 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 V

Dos testes de backup

Art. 30. Os **backups** serão verificados periodicamente visando analisar logs, identificar erros e realizar ações corretivas com o intuito de reduzir os riscos associados.

Art. 31. Os testes de restauração dos **backups** devem ser realizados, por amostragem mensalmente, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar **backups** bem-sucedidos.

Art. 32. Verificar se foram atendidos os níveis de serviço pactuados, tais como os **Recovery Time Objective – RTOs**.

Art. 33. Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do **backup** e se o procedimento foi concluído com sucesso.

Art. 34. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pelo Comitê de Tecnologia da Informação da FUNAG.

Seção VI

Dos procedimentos de restauração de backup

Art. 35. O atendimento de solicitações de restauração de arquivos, e-mails e demais formas de dados obedecerá às seguintes orientações:

I - a solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através de contato formal com a Divisão de Tecnologia da Informação;

II - a restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de **backup;**

III - a solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações; e

IV - 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 IV

DAS RESPONSABILIDADES

Art. 36. O administrador de backup e a área técnica devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de **backup**.

§1º Designa-se como administrador de **backup** o Chefe da Divisão de Tecnologia da Informação da FUNAG;

§2º Fica estabelecida como equipe técnica responsável a Seção de Suporte de Tecnologia da Informação da FUNAG.

Art. 37. São atribuições do administrador de **backup**:

I - propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela organização;

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; e

VI - definir padrões, modelos, métodos e sistemas e procedimentos de **backup** e restauração de dados.

Art. 38. São atribuições da área técnica:

I - apoiar na definição dos prazos de retenção de dados junto aos gestores negociais;

II - auxiliar na definição da periodicidade das cópias de segurança junto aos gestores da informação;

III - certificar que as cópias de segurança são realizadas conforme definição dos gestores da informação;

IV - acompanhar a execução dos **backups** por meio de ferramentas de monitoramento disponíveis para esse objetivo;

V - configurar as soluções de **backup**;

VI - manter as unidades de armazenamento de **backups** preservadas, funcionais e seguras; e

VII - realizar periodicamente testes de restauração para averiguar os processos de **backup** e estabelecer melhorias.

Art. 39. 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 o resultado das restaurações solicitadas; e

III - definir a frequência de realização do **backup** (diária, semanal, mensal, anual), bem como o tipo (completo, incremental, diferencial) e o escopo (dados digitais a serem salvaguardados).

CAPÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 40. O administrador de **backup** e a área técnica elaborarão o Plano de Backup onde deverá estar documentado os processos de **backup** e de recuperação de dados.

§1º O Plano de **Backup** de que trata o caput deverá ser atualizado sempre que houver alteração, adição ou remoção do escopo de dados a serem salvaguardados, bem como nos métodos, sistemas e mídias de backup e recuperação de dados.

Art. 41. Política de **Backup** e Restauração de Dados Digitais da FUNAG poderá ser revisada a qualquer tempo, para fins de eventual atualização, quando identificada a necessidade de alteração em qualquer de seus dispositivos.

Art. 42. Casos excepcionais não abordados nesta Política serão decididos pelo Comitê de Tecnologia da Informação da FUNAG.