PORTARIA Nº 3.019/STI, DE 26 DE SETEMBRO DE 2019.

Institui a Norma Complementar nº 4, que dispõe sobre a Política de Cópia de Segurança (*Backup*) e Restauração de Dados (*Restore*) da Agência Nacional de Aviação Civil - ANAC.

O SUPERINTENDENTE DE TECNOLOGIA DA INFORMAÇÃO, considerando a deliberação da 1ª Reunião Extraordinária do Comitê de Segurança da Informação e Comunicações da ANAC realizada em 4 de outubro de 2019, e

Considerando as obrigações estabelecidas no Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

Considerando as orientações para Gestão de Segurança da Informação e Comunicações, que deverão ser implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta, contidas na Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008, e em suas Normas Complementares;

Considerando as recomendações constantes nas normas técnicas NBR ISO/IEC 27001:2006 – Sistema de Gestão de segurança da informação e NBR ISO/IEC 27002:2005 - Código de Práticas para a Gestão da Segurança da Informação;

Considerando as Instruções Normativas nº 114, de 9 de maio de 2017, que institui a Política de Gestão de Riscos Corporativos da ANAC, nº 120, de 22 de fevereiro de 2018, que institui a Política de Governança de Tecnologia da Informação e Comunicação - PGTIC da ANAC, e nº 128, de 6 de novembro de 2018, que institui a Política de Segurança da Informação e Comunicações da Agência Nacional de Aviação Civil - PoSIC/ANAC; e

Considerando o que consta do processo 00058.036878/2019-36,

RESOLVE:

Art. 1º Instituir a Norma Complementar que disciplina a Política de Cópia de Segurança (*Backup*) e Restauração de Dados (*Restore*) da Agência Nacional de Aviação Civil - ANAC, nos termos do anexo.

Parágrafo único. A presente Política se aplica no âmbito da Agência, alcançando todos os integrantes de seu Quadro Funcional e todos os recursos administrativos e tecnológicos relacionados, de modo permanente ou temporário, à ANAC.

Art. 2º Ficam revogados:

I - a Portaria nº 3.547/STI, de 20 de novembro de 2018, publicada no Boletim de Pessoal e Serviço - BPS v.13, nº 47, de 23 de novembro de 2018; e

II - Portaria nº 794/STI, de 13 de março de 2019, publicada no Boletim de Pessoal e Serviço - BPS v.14, nº 11, de 15 de março de 2019.

Publicado no Boletim de Pessoal e Serviço - BPS v.14, nº 47, de 22 de novembro de 2019.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

GUSTAVO SANCHES

ANEXO À PORTARIA Nº 3.019/STI, DE 26 DE SETEMBRO DE 2019.

NORMA COMPLEMENTAR Nº 4.

GESTÃO DE CÓPIA DE SEGURANÇA

CAPÍTULO I
DAS DEFINIÇÕES

Art. 1º Para os fins desta Portaria, consideram-se:

I - administrador de sistema: administradores de serviços ofertados ou hospedados pela ANAC (bancos de dados, sistemas operacionais, arquivos, ativos de redes etc) que podem requisitar a realização de *backup* ou a restauração de *backup* dos serviços por eles gerenciados em caso de incidentes ou desastres;

II - administrador de *backup*: analistas técnicos da ANAC responsáveis e qualificados para as tarefas de configuração dos serviços de *backup* e também da restauração em casos de desastre ou solicitação dos responsáveis pelos dados ou administradores de sistemas;

III - appliance de *backup* em disco: hardware especialmente desenvolvido para armazenar dados de *backup* em discos usualmente com desduplicação embutida;

IV - *backup*: cópia de dados de um dispositivo de armazenamento para outro para que possa ser restaurado em caso da perda dos dados originais;

V - *backup* completo: todos os dados são copiados durante o procedimento do *backup*;

VI - *backup* incremental: somente os arquivos novos ou modificados desde a última execução do procedimento de *backup* são copiados;

VII - *backup* "*off-site*": localidade de armazenamento de *backup* diversa da origem dos dados;

VIII - curador: servidor público, designado pelo superintendente ou chefe de unidade, com a responsabilidade de gerenciar ativos de informação específicos, conforme definição da Política de Governança de Informações Digitais da ANAC;

IX - *downtime*: tempo em que os dados ficam indisponíveis;

X - IEC: *International Electrotechnical Commission;*

XI - ISO: *International Organization for Standardization;*

XII - mídia: meio físico no qual efetivamente armazenam-se os dados de um *backup*;

XIII - NBR: normatização técnica brasileira elaborada pela Associação Brasileira de Normas Técnicas - ABNT;

XIV - PST: arquivo gerado pelo sistema de correio eletrônico para armazenamento de mensagens localmente na estação de trabalho do usuário;

XV - *Recovery*: retorno de dados ou serviços ao estado original (anterior ao evento que origina a indisponibilidade de dados ou serviços);

XVI - *Recovery Time Objective* - RTO: tempo necessário para a restauração de cópias de segurança dos sistemas de informação;

XVII - *Recovery Point Objective* - RPO: quantidade de informação que poderá ser perdida no caso de uma situação de desastre;

XVIII - restauração: restauração de dados a partir de um *backup* funcional armazenado;

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

XX - *staging* de dados: modalidade de *backup* dividida em duas etapas que são armazenados em meios diferentes (geralmente disco e fita).

CAPÍTULO II
DOS OBJETIVOS

Art. 2º Constituem objetivos desta Política:

I - estabelecer as diretrizes para a realização de cópia de segurança (*Backup*) e de restauração dos dados (*Restore*) corporativos ou que são custodiados pela ANAC, visando assegurar a segurança das informações, conforme as propriedades de confidencialidade, integridade e disponibilidade dos ativos de informação;

II - definir estratégias e orientações para a implementação de controles relativos a cópias de segurança e restauração de dados da rede computacional da ANAC; e

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

CAPÍTULO III
DA ESTRATÉGIA E DAS ORIENTAÇÕES

Art. 3º As ações de Tecnologia da Informação deverão alinhar-se à estratégia institucional e às melhores práticas, observada a seguinte estratégia geral de *Backup* e *Restore*:

I - o serviço de *backup* deverá ser orientado para a restauração das informações no menor tempo possível, principalmente nos casos de indisponibilidade de serviços que dependam da operação de *Restore*;

II - os recursos adequados para a geração dos *backup*s precisam ser disponibilizados para assegurar que todos os dados e aplicações essenciais possam ser recuperados após um incidente/desastre;

III - o administrador de sistemas, o administrador de *backup* e a STI deverão estar sempre atualizados em relação às informações geradas pelo processo de *backup* e restauração;

Parágrafo único. A estratégia de que trata o caput basear-se-á em 3 (três) etapas:

I - catalogação dos servidores de dados (banco de dados / aplicações / serviços);

II - levantamento dos requisitos dos ambientes;

III - implementação do processo de *Backup* e *Restore*;

Art. 4º As ações de Tecnologia da Informação relativas ao *Backup* e *Restore* de dados deverão seguir as seguintes orientações:

I - a administração dos *backup*s deverá ser orientada para que seus trabalhos respeitem as janelas de execução, inclusive prevendo a ampliação da capacidade dos dispositivos de armazenamento;

II - os dispositivos de armazenamento dos *backup*s (fitas ou *appliance* de *backup* em disco), dos sistemas classificados como críticos, deverão ser acondicionados em ambiente com estrutura obediente à norma ABNT NBR ISO/IEC 27002:2005, em localidade diversa da origem dos dados (*backup* "*off-site*");

III - a distância mínima desejável entre os ambientes de armazenamento dos dados e as cópias de segurança deverá ser suficiente para escapar dos danos de um desastre ocorrido no local principal;

IV - as mídias defeituosas ou inservíveis serão encaminhadas para picotamento, incineração, procedimentos de sobrescrita de dados remanescentes (disco rígido) ou outro procedimento que impossibilite a recuperação dos dados por terceiros;

V - 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;

VI - 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;

VII - os administradores de sistemas em conjunto com os administradores de *backup* deverão realizar testes periódicos de restauração, no intuito de averiguar os processos de *backup* e estabelecer melhorias;

VIII - 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;

IX - o *backup* não englobará a cópia das caixas de mensagens eletrônicas armazenados em PST, em pastas do MS-Outlook (PST) na própria estação de trabalho, as quais não estarão disponíveis para recuperação, em caso de perda temporária ou definitiva do arquivo; e

X - as ações de Tecnologia de Informação que envolvam a geração de cópias de segurança e a restauração de dados deverão vincular-se às boas práticas derivadas da observância dos normativos internos e externos.

CAPÍTULO IV
DOS PAPÉIS E COMPETÊNCIAS

Art. 5º A execução da Política de Cópia de Segurança e Restauração de Dados da ANAC pautar-se-á na definição e distribuição de competência e responsabilidades entre as unidades organizacionais da Agência e será composto pelos seguintes agentes:

I - Comitê de Segurança da Informação e Comunicações;

II - Superintendência de Tecnologia da Informação - STI;

III - Curadores.

Parágrafo único. Os processos de *backup* e *Restore* dos dados gerados ou sob a guarda da ANAC deverão envolver os gestores de soluções de Tecnologia da Informação e Comunicação - TIC.

Art. 6º O alinhamento da governança de TIC às estratégias e diretrizes relacionadas à cópia de segurança e restauração de dados da ANAC é de responsabilidade do Comitê de Segurança da Informação e Comunicações e operacionalizadas pela Superintendência de Tecnologia da Informação - STI e pelo curador, que prestarão àquela todo o suporte necessário à tomada de decisão dos processos de *backup* e restauração objeto desta Portaria.

Art. 7º Compete ao Comitê de Segurança da Informação e Comunicações:

I - aprovar diretrizes referentes a ações e projetos de *backup* e *Restore* dos dados gerados ou sob a guarda da ANAC;

II - avaliar e decidir sobre questões de segurança vinculadas às cópias de segurança, respeitando o disposto na Política de Segurança da Informação e Comunicações - PoSIC; e

III - avaliar a aderência das ações do monitoramento com as diretrizes estabelecidas.

Art. 8º Compete à STI:

I - promover treinamentos e certificações necessárias para os servidores envolvidos nas atividades descritas nesta Política;

II - propor a alocação de recursos orçamentários destinados à gestão e prospecção de soluções de *backup* e *Restore* dos dados gerados ou sob a guarda da ANAC;

III - estabelecer, por meio de portaria, as regras para a gestão das cópias de segurança e restauração de dados;

IV - prevenir contra divulgação não autorizada, modificação, remoção ou destruição dos dados armazenados nos *backup*s;

V - elaborar e publicar o Plano de Comunicação de Falhas de *Backup*;

VI - elaborar e publicar o Plano de Recuperação de Incidentes de *Backup*;

VII - manter os ambientes de desenvolvimento, homologação e de produção disponíveis e atualizados para uso constante;

VIII - elaborar o catálogo dos servidores e aplicações de *backup* existentes, mediante levantamento detalhado do cenário atual da solução de *backup*, que inclua inventário dos ativos disponíveis para armazenamento, servidores envolvidos nos processos de *backup* e softwares utilizados, com a finalidade de se ter conhecimento dos riscos aos quais os dados estão sujeitos, os problemas e demais não conformidades encontradas;

IX - relacionar todo e qualquer dispositivo que pertença à ANAC e que armazene dados a ser considerado para fins de realização de cópias de segurança;

X - identificar os responsáveis pelos dados de cada sistema de informação da ANAC;

XI - projetar e aplicar proteção física contra incêndios, enchentes, explosões, perturbações da ordem pública e outras formas de desastres naturais ou que possam ser causados pelas pessoas;

XII - assegurar que as informações recebam um nível adequado de proteção;

XIII - definir um período de retenção das cópias dos logs de auditoria das operações de *backup*, para fins de futuras investigações e monitoramento de controle de acesso das ferramentas de *backup* e restauração;

XIV - armazenar as cópias de segurança dos sistemas classificados como críticos em uma localidade remota a uma distância mínima, a ser definida em normas complementares, que seja segura para escapar dos danos de um desastre ocorrido no local principal;

XV - estabelecer o perímetro de segurança do local escolhido para armazenamento das cópias de segurança;

XVI - mitigar os riscos de possíveis acessos às mídias descartadas;

XVII - manter as cópias de segurança em conformidade com os requisitos legais pertinentes;

XVIII - respeitar todos os prazos e tipos de *backup* que tenham implicações legais para os negócios e para a imagem da ANAC;

XIX - manter as cópias dos arquivos corporativos que assegurem a continuidade das operações dos processos de trabalho de cada Unidade Organizacional;

XX - disponibilizar uma área externa ao ambiente de armazenamento onde os dados estão instalados;

XXI. disponibilizar uma área para *staging* de dados, que seja externa ao ambiente de armazenamento (*storage* principal) para validação e posterior cópia para fitas;

XXII - definir o processo para o descarte dos dispositivos de armazenamento que contenham dados fora do prazo de retenção;

XXIII - mapear os servidores e as aplicações e registrar no inventário de ativos de informação;

XXIV - definir o tempo máximo de recuperação (*Recovery*) dos serviços ofertados e hospedados, consonante aos Níveis Mínimos de Serviços Exigidos - NMSE do Catálogo de Serviços da ANAC firmados junto às empresas prestadoras de serviços;

XXV - realizar testes de restauração em periodicidade a ser definida, ou mediante solicitação no Portal de Serviços da ANAC; e

XXVI - submeter ao CSIC, quando necessário, o cumprimento das diretrizes estabelecidas nesta Política.

Parágrafo único. A STI designará administrador de sistemas e administrador de *backup* e restauração de dados no intuito de operacionalizar as orientações contidas nesta Política.

Art. 9º Compete ao curador de que trata a Instrução Normativa nº 115, de 14 de agosto de 2017:

I - realizar a gestão das informações dos sistemas de informação da sua Unidade Organizacional;

II - classificar o nível de criticidade de cada aplicação;

III - classificar as informações de acordo com normativos, premissas institucionais e requisitos de negócio;

IV - definir o tempo de retenção das cópias de segurança, segundo a legislação pertinente, quando houver previsão legal, em alinhamento com as premissas institucionais ou requisitos de negócio;

V - autorizar o acesso aos dados dos sistemas de informação e às cópias de segurança e suas restaurações;

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

VII - definir o tempo necessário para a restauração de cópias de segurança dos sistemas de informação (RTO);

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

IX - solicitar a restauração de cópia de segurança, quando for necessário;

X - 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 off-line;

XII - preencher o Termo de Descarte de Mídias; e

XIII - fornecer as informações sobre os requisitos legais de cada sistema de informação sob a sua gestão.

Parágrafo único. As responsabilidades atribuídas ao curador poderão ser desempenhadas pelos gestores de sistemas, enquanto não houver designações formalizadas.

Art. 10. Compete a todos os usuários reportar à STI:

I - os incidentes na rede computacional da ANAC, que afetem a segurança das cópias de segurança, e

II - qualquer descumprimento desta Política.

Art. 11. Compete à Comissão Permanente de Avaliação de Documentos - CPAD gerenciar as informações definidas pelo responsável pelos dados.

Art. 12. As solicitações de restauração de dados deverão ser abertas pelo responsável pelos dados ou pelo administrador de sistema, em conformidade com os tempos de RTO acordados, através do Portal de Serviços da ANAC contendo os nomes e datas dos arquivos e as pastas que deverão ser recuperados.

CAPÍTULO VIII
DAS ATUALIZAÇÕES

Art. 13. Esta Norma 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.

CAPÍTULO IX
DAS DISPOSIÇÕES FINAIS

Art. 14. Em casos de quebra de segurança das cópias armazenadas ou no processo de execução, a STI deverá ser imediatamente acionada para adotar as providências necessárias, podendo, inclusive, determinar a restrição temporária ao acesso aos recursos computacionais envolvidos no processo de cópias de segurança e restauração dos dados corporativos da ANAC.

Art. 15. Os casos omissos serão resolvidos pelo Comitê de Tecnologia da Informação e Comunicações apoiado pelo Comitê de Segurança da Informação e Comunicações da ANAC quando for necessário.