MINISTÉRIO PÚBLICO FEDERAL
SECRETARIA GERAL

INSTRUÇÃO NORMATIVA SG/MPF Nº 3, DE 6 DE MARÇO DE 2023.

Dispõe sobre a institucionalização da Política de cópia de segurança (backup) e restauração de dados digitais no âmbito do Ministério Público Federal.

A SECRETÁRIA-GERAL DO MINISTÉRIO PÚBLICO FEDERAL, no uso da atribuição conferida no art. 6º, inciso V, do Regimento Interno Administrativo do Ministério Público Federal (RIA/MPF), aprovado pela Portaria SG/MPF nº 382, de 5 de maio de 2015, e, tendo em vista o que consta no Memorando nº 276/2023/STIC (PGR-00075104/2023);

Considerando o objetivo estratégico de prover soluções tecnológicas integradas, sustentáveis e estáveis, com foco na segurança da informação, na simplicidade e na necessidade dos usuários;

Considerando a necessidade de minimizar os riscos e enfrentar ameaças associadas a perdas de dados, favorecendo a continuidade de negócios e a recuperação de desastres;

Considerando a Política e o Plano de Segurança Institucional do Ministério Público Federal;

Considerando o disposto na Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD);

Considerando o Acórdão nº 1109/2021, do Plenário do Tribunal de Contas da União, que recomenda a aprovação formal e a atualização das políticas gerais e planos específicos de cópias de segurança (backup);

Considerando a auditoria no processo Gerenciamento da Continuidade, iniciada com a Solicitação de Auditoria nº 3/2021/DITIC/DAINF/AUDIN-MPU (AUDIN-MPU-00000513/2021), que identificou a necessidade de atualização da política/plano de backup;

Considerando a Política de Gestão de Riscos do Ministério Público da União, instituída pela Portaria PGR/MPU nº 78, de 8 de agosto de 2017;

Considerando a Portaria PGR/MPF nº 155, de 24 de março de 2022, que dispõe sobre a Gestão de Riscos no Ministério Público Federal e aprova o Plano de Gestão de Riscos do Ministério Público Federal;

Considerando a Política Nacional de Tecnologia da Informação do Ministério Público (PNTI-MP), instituída pela Resolução CNMP nº 171, de 27 de junho de 2017; e

Considerando as boas práticas de Segurança de Tecnologia da Informação, notadamente as normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013 e os guias NIST Cybersecurity Framework Subcategory e CIS Critical Security Controls, resolve:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Fica Instituída a Política de cópia de segurança (backup) e restauração de dados digitais do Ministério Público Federal - MPF.

Art. 2º A Política de cópia de segurança (backup) e restauração de dados digitais do MPF objetiva instituir diretrizes, responsabilidades e competências que visam garantir a segurança, confidencialidade, integridade e disponibilidade dos dados digitais custodiados pela área de tecnologia da informação e comunicação (TIC) do MPF.

Art. 3º A implantação desta política busca minimizar os impactos decorrentes da perda de dados, seja por falha humana, por falha de equipamentos tecnológicos, ataques cibernéticos, catástrofes naturais ou outras ameaças, bem como reduzir ao máximo o tempo de parada dos serviços de TIC.

Art. 4º Esta Política aplica-se a todos os serviços de TIC, em uso e de propriedade do MPF, no âmbito de todas as unidades que compõem o MPF.

Art. 5º Os serviços de TIC críticos do MPF devem ser formalmente definidos na Política de Gestão de Continuidade de Negócios ou instrumento equivalente definido pela Comissão Estratégica de Tecnologia da Informação do MPF.

Parágrafo único. Independentemente da definição prevista no caput, fica estabelecido o Sistema Único como crítico para o MPF.

CAPÍTULO II
DOS CONCEITOS

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

I - Área técnica: unidade responsável pela operação técnica dos ativos e serviços de tecnologia da informação e comunicação (TIC);

II - Área de administração de banco de dados: unidade responsável pela administração e operação dos sistemas gerenciadores de banco de dados;

III - Processos ou atividades críticas: tarefas essenciais para a continuidade e a manutenção das operações do Ministério Público Federal, cuja interrupção, parada ou falha afeta de forma significativa a atuação institucional;

IV - Ativo: aquilo que tem valor – tangível ou intangível - para a organização (tais como informação, softwares, equipamentos, instalações, serviços, pessoas e a imagem institucional);

V - Backup: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação em caso de perda dos originais;

VI - Backup Completo (Full): modalidade de backup em que todos os dados a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma mídia de backup, independentemente de terem sido ou não alterados desde o último backup;
VII - Backup Diferencial: modalidade de backup em que são salvaguardados apenas dados novos ou modificados desde o último backup completo efetuado;

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

IX - Backup on-line: uma vez realizado, o backup é acessível dentro da rede de dados do MPF;

X - Backup off-line: uma vez realizado, o backup não é acessível em rede, sendo armazenado em mídias físicas removíveis;

XI - Backup off-site: uma vez realizado, o backup é armazenado em localidade diversa da origem dos dados, geograficamente separado, podendo também ser realizado por meio de serviço de backup em nuvem;

XII - Base de dados ou banco de dados: coleção de dados inter-relacionados, armazenando informações sobre um domínio específico;

XIII - Código fonte: é o conjunto de palavras ou símbolos escritos de forma ordenada, contendo instruções em uma linguagem de programação, de maneira lógica;

XIV - Criticidade: grau de importância da informação para a continuidade das atividades e serviços;

XV - Custódia: consiste na responsabilidade de se guardar um ativo para terceiros, não permitindo automaticamente o acesso ao ativo e nem o direito de conceder acesso a outros;

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

XVII - Data at rest: são dados que não estão se movendo ativamente de dispositivo para dispositivo ou rede para rede, como dados armazenados em um disco rígido, laptop, unidade flash ou arquivados/armazenados de alguma outra forma;

XVIII - Data in transit: são dados que se movem ativamente de um local para outro, como pela Internet ou por meio de uma rede privada;

XIX - Descarte: eliminação adequada dos dados, mídias de backup e acervos digitais;

XX - Disponibilidade: garantia de que o dado esteja acessível e utilizável sob demanda de pessoa ou entidade devidamente autorizada;

XXI - Equipe administradora de backups: equipe responsável pelos procedimentos de configuração, execução, monitoramento, elaboração de padrões, atendimentos avançados, resolução de incidentes relacionados ao backup, coordenação dos testes dos procedimentos de backup e restauração;

XXII - Gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem, fornecendo uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

XXIII - Gestor da informação: agente público responsável pela definição de requisitos do serviço de TIC e pelas informações produzidas em seu processo de trabalho, ou seja, deve ser um gestor da área negocial ou da área de tecnologia da informação e comunicação, conforme o caso;

XXIV - Incidente: evento, 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, sequestro, 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;

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

XXVI - Janela de backup: intervalo de tempo durante o qual as cópias de segurança sob execução agendada ou manual poderão ser executadas;

XXVII - Log ou registro de auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional, para posterior análise, podendo ser gerado por sistemas operacionais, aplicações, entre outros;

XXVIII - Máquinas virtuais: é um recurso de computação que utiliza software ao invés de um computador físico para executar programas e aplicativos de forma que um ou mais “visitantes” virtuais executam numa mesma máquina física “hospedeira” e que cada máquina virtual executa seu próprio sistema operacional e funciona separada das outras máquinas virtuais;

XXIX - Mídia: mecanismos em que dados podem ser armazenados - inclui discos ópticos, magnéticos, CDs, fitas e papel, entre outros;

XXX - Nuvem: uma vasta rede de servidores remotos ao redor do globo que são conectados e operam como um único ecossistema de modo que 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;

XXXI - Operador de backup: agente responsável por procedimentos de atendimento de primeiro nível, acompanhamento de execução de rotinas de backup, realização de restaurações de arquivos de usuários, manuseio das bibliotecas de fitas, abastecimento de fitas na biblioteca durante as execuções dos backups, guarda das mídias gravadas nos cofres de armazenamento e gerenciamento de estoque de fitas locais;

XXXII - Plano de backup: documento 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;

XXXIII - Repositório de arquivo: conjunto de documentos ou local onde os documentos são guardados;

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

XXXV - Rotina de backup: procedimentos de realização de cópias de segurança;

XXXVI - Recovery Point Objective (RPO): ponto no tempo em que os dados dos serviços de TIC podem ser recuperados com sucesso após uma situação de parada ou perda, admitindo-se a perda dos dados gerados após esse ponto no caso de um incidente, pois corresponde à quantidade máxima aceitável de dados que se admite perder;

XXXVII - Recovery Time Objective (RTO): tempo estimado para restaurar os dados e tornar os serviços de TIC novamente operacionais, correspondendo ao prazo máximo

em que se admite manter os serviços de TIC inoperantes até a restauração de seus dados, após um incidente;

XXXVIII - Serviço de TIC: sistema de informação ou qualquer solução de tecnologia da informação e comunicação que armazene informações em formato digital, incluindo bases de dados e repositórios de arquivos institucionais;

XXXIX - Serviço de TIC crítico: serviço de TIC que suporta os processos ou atividades críticas;

XL - Servidor: computador de alta capacidade que faz parte de uma rede corporativa, e que fornece serviços a outros computadores.

CAPÍTULO III

DOS PLANOS DE BACKUP

Art. 7º Para todos os serviços de TIC classificados como críticos em uso no MPF, deve haver um plano de backup, conforme modelo a ser incluído no sistema de registro, tramitação e armazenamento de documentos do MPF, devidamente formalizado em documento administrativo e assinado pelo:

I - gestor da informação;

II - área técnica;

III - área administradora de banco de dados quando aplicável; e

IV - equipe administradora de backups.

Art. 8º Para todos os serviços de TIC não críticos em uso no MPF, deve haver um plano de backup simplificado, devidamente registrado pelo gestor da informação no sistema de registro de chamados em uso no MPF, seguindo modelo de pedido na categoria "Infraestrutura de TIC - Inclusão de plano de backup simplificado".

Art. 9º Serão permitidos planos de backup de serviços não críticos agrupados por categorias ou conjuntos de serviços e ativos.

Parágrafo único. O agrupamento só será permitido se os serviços ou ativos abrangidos possuírem os mesmos requisitos de salvaguarda e restauração de dados digitais.

Art. 10. Os planos de backup devem ser revisados periodicamente, no mínimo em intervalos anuais, ou quando houver mudanças significativas que os influenciem.

Art. 11. Os planos de backup dos dados referentes aos serviços de TIC críticos e aos serviços de TIC não críticos devem refletir 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, e devem explicitar, no mínimo, os seguintes requisitos técnicos:

I - escopo (dados digitais a serem salvaguardados, com apontamento do local), incluindo:

a) código fonte;

b) base de dados;

c) repositório de arquivos;

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

e) máquinas virtuais;

f) ambientes abrangidos (produção, homologação, desenvolvimento, etc);

g) arquivos de logs.

II - modalidade de backup: definindo se será completo, diferencial ou incremental. Poderá ser uma associação destes;

III - frequência temporal de realização do backup: definindo se será diário, semanal ou mensal. Poderá ser uma associação destes;

IV - 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), deve ser definido com base na criticidade, frequência da atualização dos dados e características específicas de cada serviço de TIC;

V - RPO; e

VI - RTO.

Art. 12. Não serão salvaguardados nem recuperados dados armazenados localmente, nas estações de trabalho dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas áreas técnicas do MPF.

Art. 13. A salvaguarda dos dados em formato digital pertencentes a serviços de TIC do MPF, 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.

§ 1º Para todos os serviços de TIC classificados como críticos custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve ser dada preferência para mecanismos de salvaguarda off-line e off-site em território brasileiro.

§ 2º Os acordos devem prezar pela confidencialidade dos dados custodiados e atendimento às necessidades específicas do serviço, devendo ser registrados a estratégia e mecanismos de backup adotados em plano próprio de cada serviço.

CAPÍTULO IV

DOS PADRÕES OPERACIONAIS

Seção I

Dos princípios gerais

Art. 14. A política de cópia de segurança (backup) e restauração de dados digitais deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional, devidamente amparados nas estratégias de governança de TIC do MPF.

Art. 15. 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 TIC.

Art. 16. As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TIC ou dado salvaguardado, dando prioridade aos serviços de TIC críticos da organização.

Art. 17. Os backups devem ser armazenados (data at rest) e transmitidos (data in transit) de forma criptografada, considerando as melhores práticas de mercado e normas vigentes.

Art. 18. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup, definido por cada área técnica.

Seção II

Das ferramentas de backup

Art. 19. As rotinas de backup devem utilizar soluções dedicadas e especializadas para este fim, preferencialmente de forma automatizada.

Art. 20. Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização e devem possuir plano de backup próprio documentado.

Parágrafo único. Compete à Secretaria de Tecnologia da Informação e Comunicação - STIC adquirir e manter o parque de ativos envolvidos no processo de backup sempre atualizado e compatível com a demanda do MPF.

Seção III

Da frequência e retenção dos backups

Art. 21. Os backups dos serviços de TIC do MPF devem ser realizados utilizando-se as seguintes frequências temporais:

I - diária, preferencialmente de segunda a sexta-feira;

II - semanal, preferencialmente nos finais de semana; e

III - mensal, preferencialmente no primeiro final de semana de cada mês.

Art. 22. Especificidades dos serviços de TIC podem demandar frequência e tempo de retenção diferenciados, que devem estar devidamente registrados no plano de backup.

Art. 23. Os serviços de TIC críticos do MPF devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

I - diária: 2 (dois) meses;

II - semanal: 12 (doze) semanas; e

III - mensal: 3 (três) anos.

Art. 24. Os serviços de TIC não críticos do MPF devem ser resguardados observando-se o padrão mínimo de correlação

frequência/retenção de dados estabelecida a seguir:

I - diária: 1 (um) mês;

II - semanal: 6 (seis) semanas; e

III - mensal: 2 (dois) anos.

Art. 25. O padrão mínimo de modalidade de backup deve observar a correlação frequência/tipo de cópia estabelecida a seguir:

I - diária: incremental;

II - semanal: completo;

III - mensal: completo.

Art. 26. Os backups devem ter no mínimo duas cópias, realizadas em formatos de mídia distintos, sendo um on-line e outro off-line.

§ 1º Os serviços de TIC classificados como críticos devem contar com backups em mídias off-line e off-site que devem ser realizados no mínimo semanalmente;

§ 2º Para serviços não críticos a cópia off-line deve ser realizada no mínimo mensalmente;

Art. 27. A recuperação de dados não será viável em caso de perdas anteriores à conclusão da cópia de segurança.

Art. 28. Todo serviço de TIC a ser descontinuado deve ser submetido a um backup completo e sua retenção deve ser de, no mínimo, um ano.

Art. 29. O backup dos logs de ativos de segurança de rede do MPF deve ser retido por 5 (cinco) anos.

Art. 30. A adoção de frequências e tempos de retenção distintos dos definidos nesta seção deve ser fundamentada no plano de backup, cabendo avaliação da equipe administradora de backups quanto à viabilidade.

Seção IV

Do uso da rede

Art. 31. A equipe administradora de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do MPF, garantindo que o tráfego necessário às suas atividades não implique em impacto demasiadamente negativo ao desempenho dos demais serviços de TIC.

Parágrafo único. A equipe administradora do backup, considerando as limitações técnicas e orçamentárias, deve dar preferência a soluções que desonerem a rede de dados do MPF.

Art. 32. O acesso à plataforma de gerência da solução de backup deve ser isolada em nível de rede, com permissões exclusivas para

a equipe administradora de backup e operadores.

Seção V

Do armazenamento e descarte das mídias de backup

Art. 33. As mídias de backup 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 mídia de backup; e

VI - a vida útil da mídia de backup.

Art. 34. A equipe administradora 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. 35. Poderão ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de recuperação dos dados seja considerado aceitável pelos gestores das informações.

Art. 36. 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 (físico e lógico) a pessoas autorizadas pela equipe administradora de backup.

§ 1º O local de armazenamento dos backups off-line não pode ser o mesmo dos dados originais.

§ 2º O acesso aos locais deve ser controlado eletronicamente utilizando duplo fator de autorização e os registros de acesso devem ser guardados.

§ 3º As mídias de backups off-line devem obrigatoriamente ser armazenadas em cofres anti-chamas certificados.

§ 4º O acesso lógico às mídias de backup deve ser segregado de outros equipamentos e serviços na rede, limitando-se o acesso direto por ferramentas de backup utilizadas para realização das atividades de cópia ou restauração.

Art. 37. As mídias de backup off-line devem ser etiquetadas, contendo o código de identificação.

Art. 38. Após o tempo de retenção definido no plano de backup, fica autorizado o descarte ou o reaproveitamento de mídia de backup.

Parágrafo único. O descarte de mídias, devido à obsolescência tecnológica ou defeito irrecuperável, deve ocorrer de forma segura, protegida, sustentável e ambientalmente correta; por meio de trituração, quebra, execução de procedimentos de sobrescrita de dados remanescentes (disco rígido) ou outro procedimento que impossibilite a recuperação dos dados por terceiros.

Seção VI

Dos testes de restauração de backup

Art. 39. Os backups devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

Art. 40. Os testes de restauração dos backups devem ser realizados em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis.

Parágrafo único. Os testes devem utilizar os diferentes tipos de mídias de backup.

Art. 41. Os testes de restauração dos backups se dividem nas seguintes categorias:

I - Testes básicos de restauração: objetivam assegurar a disponibilidade e integridade dos dados, validando o RPO frente ao definido no plano de backup.

II - Testes de base de dados: objetivam assegurar que as cópias de segurança de base de dados podem ser efetivamente restauradas para uma instância de base de dados.

III - Testes completos: objetivam testar o serviço de forma completa, incluindo todos os elementos previstos no plano de backup para uma efetiva recuperação do serviço, medindo-se o tempo de restauração para fins de comparação com o RTO previsto no plano de backup. Devem utilizar preferencialmente mídias off-line para restauração e estimativa do RTO no pior cenário.

Art. 42. Os testes básicos de restauração dos serviços de TIC e os testes de restauração de bases de dados devem ser realizados nos seguintes intervalos mínimos:

I - trimestralmente, para todos os serviços de TIC críticos; e

II - mensalmente, por amostragem, para serviços de TIC não críticos.

Art. 43. Os testes de restauração completos dos serviços de TIC devem ser realizados no mínimo:

I - anualmente, para todos os serviços de TIC críticos; e

II - anualmente, por amostragem, para os serviços de TIC não críticos.

Parágrafo único. Os testes completos devem ser planejados e executados por equipe composta no mínimo por operador de backup, integrante da área técnica, integrante da área de administração de banco de dados e gestor da informação.

Art. 44. Os testes de restauração devem ser automatizados, sempre que possível.

Seção VII

Dos indicadores operacionais de backup

Art. 45. As rotinas de backup devem ser monitoradas através de indicadores próprios, visando ao acompanhamento contínuo pela equipe administradora do backup, gestores da informação e áreas técnicas, de forma que esses indicadores devem contemplar no mínimo:

I - resultado do backup diário, semanal e mensal por serviço de TIC;

II - resultado do último teste realizado por serviço de TIC e por tipo de teste;

III - percentual de backups com resultado normal num dado intervalo de tempo; e

IV - percentual de testes de backup com resultado normal num dado intervalo de tempo.

Art. 46. Os indicadores devem ser mantidos em série histórica para fins de comparação e análise de tendências.

Art. 47. Indicadores adicionais podem ser propostos através dos planos de backup.

Seção VIII

Da Restauração de Dados

Art. 48. A solicitação de restauração de dados que tenham sido salvaguardados deve ser realizada por meio da abertura de chamado no sistema de registro de chamados em uso no MPF, e depende de autorização do respectivo gestor da informação.

Art. 49. A solicitação deve conter as informações suficientes para permitir a restauração, tais como: nomes dos sistemas ou serviços, arquivos e/ou pastas que devem ser recuperados, a data do arquivo que se pretende ter acesso e se a restauração deve sobrescrever o dado atual ou se será feita em um local diferente do original.

CAPÍTULO V

DAS RESPONSABILIDADES

Art. 50. A equipe administradora de backup e o operador de backup devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de armazenamento e backup.

Art. 51. São atribuições da equipe administradora de backup:

I - propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pelo MPF;

II - providenciar a criação e manutenção dos backups;

III - configurar as soluções de backup;

IV - manter as mídias de backups preservadas, funcionais e seguras;

V - definir os procedimentos de restauração e neles auxiliar;

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

VII - tomar medidas preventivas para evitar falhas;

VIII - reportar imediatamente à chefia imediata os incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de backups;

IX - gerenciar mensagens e registros de auditoria de execução dos backups, em busca de erros, durações anormais e oportunidades de melhoria do desempenho do backup;

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

XI - propor modificações visando ao aperfeiçoamento da Política de cópia de segurança (backup) e restauração de dados digitais do MPF;

XII - coordenar a execução dos testes de restauração e analisar os relatórios de execução;

XIII - propor e acompanhar os indicadores operacionais de backup;

XIV - elaborar planos de backup para os ativos de TIC sob sua administração técnica direta;

XV - apoiar a equipe de administração de banco de dados no planejamento e operação de rotinas e testes dos backups de base de dados; e

XVI - sugerir à chefia imediata os indicados para desempenhar o papel de operadores de backup.

Art. 52. São atribuições do operador de backup:

I - restaurar os backups em caso de necessidade;

II - operar e manusear as mídias de backups;

III - informar a equipe administradora de backup qualquer problema que impossibilite a criação ou restauração de um backup;

IV - executar os testes básicos de restauração de backup; e

V - alimentar os indicadores operacionais de backup.

Art. 53. São atribuições da área de administração de banco de dados:

I - informar a equipe administradora de backup qualquer problema que impossibilite a criação ou restauração de um backup de base de dados;

II - sanar dúvidas técnicas da equipe administradora de backup acerca das informações salvaguardadas;

III - executar os testes de base de dados restauradas e validar, tecnicamente, o resultado das restaurações e testes;

IV - propor e alimentar os indicadores operacionais de backup relacionados a bases de dados;

V - apoiar a equipe administradora de backups e os operadores de backup no planejamento e operação de rotinas dos backups de base de dados;

VI - providenciar a criação e manutenção dos backups de base de dados na solução específica para o sistema gerenciador de base de dados que se integra à ferramenta de backup geral;

VII - restaurar os backups de base de dados em caso de necessidade; e

VIII – elaborar planos de backup para os ativos de TIC sob sua administração técnica direta.

Art. 54. São atribuições das áreas técnicas:

I - solicitar restaurações de dados, com autorização do respectivo gestor da informação;

II - sanar dúvidas técnicas da equipe administradora de backup acerca das informações salvaguardadas;

III - validar, em parceria com o gestor da informação, o resultado das restaurações eventualmente solicitadas;

IV - validar, em parceria com o gestor da informação, o resultado dos testes de restauração dos backups; e

V - elaborar planos de backup para os ativos de TIC sob sua administração técnica direta.

Art. 55. São atribuições dos gestores da informação:

I - solicitar, formalmente, a salvaguarda das informações sob sua responsabilidade;

II - autorizar as solicitações de recuperação de dados realizadas pela área técnica;

III - validar, em parceria com a área técnica, o resultado das restaurações eventualmente solicitadas; e

IV - validar, em parceria com a área técnica, o resultado dos testes de restauração dos backups.

CAPÍTULO VI

DA IMPLANTAÇÃO

Art. 56. A presente Política, após sua entrada em vigor, deve ser implantada nos seguintes prazos:

I - até 3 (três) meses, para elaborar a lista de serviços de TIC, com os respectivos gestores da informação e a classificação quanto a criticidade (críticos e não críticos);

II - até 6 (seis) meses, para elaborar todos os planos de backup dos serviços críticos de TIC;

III - até 12 (doze) meses, para providenciar a implementação de todos os planos de backup dos serviços críticos de TIC;

IV - até 12 (doze) meses, para elaborar todos os planos de backup dos serviços não críticos de TIC; e

V - até 18 (dezoito) meses, para providenciar a implementação de todos os planos de backup dos serviços não críticos de TIC.

§ 1º A lista de serviços de TIC prevista no inciso I do caput deve ser atualizada sempre que necessário e revisada no mínimo a cada 12 (doze) meses.

§ 2º Os serviços de TIC que surgirem após a elaboração da lista prevista no inciso I do caput devem ter seus planos de backup implantados antes da sua entrada em produção.

§ 3º Após vencidos os prazos estabelecidos nos incisos II e IV do caput, não serão salvaguardados nem recuperados dados que não façam parte de um plano de backup formalmente definido.

§ 4º Excepcionalmente e com autorização expressa do Secretário de Tecnologia da Informação e Comunicação e do gestor da informação, será concedido prazo adicional para implantação do plano de backup após a entrada em produção do serviço de TIC.

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Art. 57. Compete ao Secretário de Tecnologia da Informação e Comunicação dirimir as dúvidas suscitadas na aplicação do disposto nesta Instrução Normativa, sendo os casos omissos decididos pelo Secretário-Geral do Ministério Público Federal.

Art. 58. Fica revogada a Instrução Normativa SG/MPF nº 1, de 2 de janeiro de 2014.

Art. 59. Esta Instrução Normativa entra em vigor em 90 (noventa) dias após a data de sua publicação.

Parágrafo único. Durante o período anterior à entrada em vigor desta Política, a Secretaria de Tecnologia da Informação e Comunicação deverá promover sua ampla divulgação junto às partes interessadas.

ELIANA PERES TORELLY DE CARVALHO