RESOLUÇÃO Nº 314-CONSAD, 14 de dezembro de 2023.

Estabelece a Norma de Backup e Restauração de Dados Digitais da Universidade Federal do Maranhão.

O Reitor da Universidade Federal do Maranhão, na qualidade de **PRESIDENTE DO CONSELHO DE ADMINISTRAÇÃO**, no uso das atribuições estatutárias e regimentais;

Considerando ainda, o que consta no Processo nº 013310/2022-16;

R E S O L V E ad referendum deste Conselho:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º A Norma de *Backup* e Restauração de Dados Digitais complementa a Política Geral de Segurança da Informação da Universidade Federal do Maranhão (UFMA) e objetiva instituir diretrizes, responsabilidades e competências que visam garantir a segurança, a integridade e a disponibilidade dos dados digitais custodiados pelos setores que utilizam serviços de Tecnologia da Informação e Comunicação (TIC) nesta Instituição e formalmente definidos como de necessária salvaguarda.

Art. 2º Esta norma aplica-se a todos os sistemas computacionais, bases de dados e repositórios de arquivos institucionais, em formato digital, em uso e de propriedade da UFMA, no âmbito do Ensino, Pesquisa, Extensão, Inovação e Administração.

Art. 3º Para todos os sistemas computacionais, bases de dados e repositórios de arquivos institucionais em uso na Rede UFMA, deve haver um plano de *backup* e restauração de dados, devidamente homologado pela Superintendência de Tecnologia da Informação por meio da Diretoria de Infraestrutura e Segurança da Informação (DISI) e pelo administrador de *backups*.

§ 1º Não serão salvaguardados nem restaurados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora do contexto de processamento de dados mantidos pela Superintendência de Tecnologia da Informação ou que não façam parte de um plano de *backup* formalmente definido, cabendo ao administrador de *backup* a prerrogativa de negar solicitações neste sentido.

§ 2º O *backup* será facultativo quando ocorrerem as seguintes situações concomitantemente:

I. O serviço for classificado como não crítico; e

II. O volume de dados gerados pelo serviço for expressivo a ponto de onerar e inviabilizar a capacidade operacional da infraestrutura existente.

Art. 4º A salvaguarda dos dados em formato digital pertencentes à UFMA, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve constar nos acordos ou contratos que formalizam a relação entre os envolvidos.

CAPÍTULO II
DOS CONCEITOS

Art. 5º Para os fins desta norma, considera-se:

I. Administrador de *backup*: pessoa responsável pelos procedimentos de configuração, execução, monitoramento, elaboração de padrões, atendimentos avançados, resolução de incidentes, testes dos procedimentos de *backup* e restauração, e designada formalmente entre os empregados ou servidores públicos ocupantes de cargo efetivo, com formação ou capacitação técnica compatível às suas atribuições;

II. Área técnica: unidade responsável pelo modelo operacional de TI da Universidade;

III. Ativo: aquilo que tem valor tangível ou intangível para organização (tais como informação, *software*, equipamentos, instalações, serviços, pessoas e imagem institucional);

IV. *Backup*: termo que representa conjunto de procedimentos de salvaguarda de dados de um sistema computacional ou de um repositório, garantindo guarda, proteção e restauração em caso de perda, com fidelidade ao original assegurada, ou termo utilizado para identificar a mídia em que a cópia é realizada;

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

VI. *Backup* diferencial: modalidade de *backup* em que são salvaguardados apenas dados novos ou modificados desde o último *backup* completo efetuado;

VII. *Backup* incremental: modalidade de *backup* na qual somente os arquivos novos ou modificados desde o último *backup* completo, diferencial ou incremental são salvaguardados;

VIII. Base de dados ou banco de dados: coleção de dados interrelacionados, armazenando informações sobre um domínio específico ou conjuntos de registros organizados que se relacionam de forma a criar algum sentido (informação) e dar eficiência durante uma consulta ou a geração de informações ou conhecimento;
IX. 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;
X. Criticidade: grau de importância da informação para a continuidade das atividades e serviços;
XI. Custódia: consiste na responsabilidade de se guardar um ativo para terceiros, contudo, a custódia não permite o acesso automático ao ativo e nem o direito de conceder acesso a outros;
XII. Dado: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;
XIII. Descarte: eliminação correta dos dados, unidades de armazenamento e acervos digitais;
XIV. Disponibilidade: garantia de que o dado esteja acessível e utilizável por pessoa ou entidade devidamente autorizada;
XV. Gestão de continuidade de negócio: processo abrangente de gestão que identifica ameaças potenciais para uma organização, os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem e que promove resiliência organizacional por meio da qual a organização é capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;
XVI. Gestor da informação: agente público responsável formalmente pela administração das ferramentas utilizadas e pelas informações produzidas em seu processo de trabalho, ou seja, deve ser um gestor da área negocial;
XVII. 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, 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 de restauração;
XVIII. Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
XIX. Janela de *backup*: intervalo de tempo durante o qual as cópias de segurança sob execução agendada ou manual poderão ser executadas;
XX. 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;

XXI. Mídia: mecanismos em que dados podem ser armazenados além da forma e da tecnologia utilizada para a comunicação, incluindo, mas não somente: discos ópticos, magnéticos, CDs, fitas e papel;
XXII. Nuvem: rede de servidores remotos ao redor do mundo que são conectados e operam como um único ecossistema e são responsáveis por armazenar e gerenciar dados, executar aplicativos ou fornecer serviços ou conteúdos, podendo ser acessados de qualquer dispositivo com acesso à Internet;
XXIII. Operador de *backup*: pessoa responsável por procedimentos de atendimento de primeiro nível, acompanhamento de execução de rotinas de *backup*, realização de restaurações de arquivos de usuários, manutenção de troca de fitas no robô e gerenciamento de estoque de fitas locais, devendo ser designado entre os empregados, servidores públicos ou terceirizados alocados na UFMA, com formação ou capacitação técnica compatível às suas atribuições.
XXIV. Plano de *backup*: documento formal onde são definidos os responsáveis pela cópia dos dados, o conteúdo armazenado, periodicidade de execução da cópia e tempo de retenção, de acordo com as orientações da norma de *backup*;
XXV. Recurso multimídia: combina sons, imagens e vídeos, que são diferentes tipos de mídia;
XXVI. Restauração de dados: processo que permite copiar os dados salvaguardados de um *backup* para o local original ou para um local alternativo;
XXVII. Repositório de arquivo: conjunto de documentos ou lugar onde os documentos são guardados;
XXVIII. Responsável técnico: pessoa da área técnica responsável por auxiliar gestor da informação na elaboração do plano de *backup* e solicitar restauração de dados com anuência do gestor da informação quando for pertinente;
XXIX. Retenção: intervalo de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração; e
XXX. Rotina de *backup*: procedimentos de realização de cópias de segurança.

CAPÍTULO III
DAS REFERÊNCIAS NORMATIVAS E DE BOAS PRÁTICAS

Art. 6º A presente norma tem como referências:
I. a Instrução Normativa GSI/PR nº 01, 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;
II. a Lei n° 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);
III. a Norma Complementar nº 09/IN01/DSIC/GSIPR (revisão 02), de 16 de julho de 2014, que estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e

Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta;

IV. a Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização;

V. a Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações;

VI. o *framework Information Technology Infrastructure Library* – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI;

VII. o *framework Control Objectives for Information and Related Technology* – Cobit, v. 5, conjunto de boas práticas a serem aplicadas à governança da TI, e

VIII. Acórdão 1.109/2021-TCU-Plenário, prolatado na Sessão Telepresencial de 12/5/2021, por meio do qual o Tribunal de Contas da União apreciou o processo em epígrafe, que trata de auditoria com vistas a avaliar a efetividade dos procedimentos de *backup* das organizações públicas federais.

CAPÍTULO IV
DOS PADRÕES OPERACIONAIS

Seção I
Dos princípios gerais

Art. 7º Esta Norma de *Backup* e Restauração de Dados Digitais deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional, devidamente amparada nas estratégias de governança de TI da UFMA.

Art. 8º 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.

Art. 9º 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.

Paragráfo Único. Para mensurar a criticidade de um serviço, sugere-se a utilização de matriz de risco (probabilidade x impacto).

Art. 10 Deve ser elaborada lista de ativos de informação com a designação do respectivo gestor da informação e sua classificação quanto à criticidade (críticos e não críticos), por meio de processo no Sistema Eletrônico de Informações (SEI) e aprovado pelo Comitê de Governança, Integridade e Transparência (CGIT).

Parágrafo Único. A Superintendência de Tecnologia da Informação (STI) deverá elaborar a lista de ativos para aprovação do CGIT.

Art. 11 Os *backups* devem estar em conformidade com a legislação vigente, em especial ao que compete à LGPD.

Art. 12 Recomenda-se que os *backups* sejam armazenados de forma criptografada, considerando as melhores práticas de mercado e normas vigentes.

Parágrafo Único. A encriptação deve ser utilizada preferencialmente em situações em que a confidencialidade seja considerada importante.

Seção II
Das ferramentas de *backup*

Art. 13 As rotinas de *backup* devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

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

Art. 14 Os ativos envolvidos no processo de *backup* são considerados ativos críticos para a organização.

Parágrafo Único. Compete à Superintendência de Tecnologia da Informação solicitar as justificativas pertinentes, os equipamentos necessários para realizar o armazenamento e o *backup* dos ativos críticos com o objetivo de garantir a segurança, a disponibilidade e a integridade dos mesmos.

Seção III
Da frequência e retenção dos dados backups

Art. 15 Os *backups* devem ser realizados utilizando as seguintes frequências temporais ou poderá ser uma associação destas:

I. diária;
II. semanal;
III. quinzenal;
IV. mensal;
V. semestral; e
VI. anual.

Parágrafo Único. A alteração das frequências definidas deve ser precedida de solicitação e justificativa formais, encaminhadas ao administrador de *backup* e sua aprovação depende da anuência do diretor máximo da área técnica.

Art. 16 Especificidades dos serviços de TI críticos e não críticos podem demandar frequência e tempo de retenção diferenciados, que devem estar devidamente registrados no plano de *backup* do sistema computacional, base de dados e repositório de arquivos.

§ 1º Os serviços de TI críticos da UFMA devem observar a correlação entre frequência e retenção de dados estabelecida a seguir:

I. diária: 1 (um) mês;
II. semanal: 4 (quatro) meses;
III. quinzenal: 6 (seis) meses;
IV. mensal: 12 (doze) meses;
V. semestral: 24 (vinte e quatro) meses; e
VI. anual: 60 (sessenta) meses.

§ 2º Os serviços de TI não críticos da UFMA devem observar a correlação entre frequência e retenção de dados estabelecida a seguir:

I. diária: 15 (quinze) dias;
II. semanal: 2 (dois) meses;
III. quinzenal: 4 (quatro) meses;
IV. mensal: 6 (seis) meses;
V. semestral: 12 (doze) meses; e
VI. anual: 24 (vinte e quatro) meses.

§ 3º A alteração dos tempos de retenção definidos deve ser precedida de solicitação e justificativa formais encaminhadas ao administrador de *backup* e sua aprovação depende da anuência do diretor máximo da área técnica.

§ 4º 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.

Art. 17 A solicitação de salvaguarda dos dados, referentes aos serviços de TI críticos e aos serviços de TI não críticos, deve ser realizada pelos responsáveis técnicos dos serviços de TI, por meio da elaboração do plano de *backup* que deve explicitar, no mínimo, os seguintes requisitos técnicos:

I. escopo: dados digitais a serem salvaguardados, com apontamento do local, tais como código-fonte, banco de dados, repositório de arquivos, arquivos de configuração de servidores e ativos de rede, máquinas virtuais e infraestrutura DevOps.
II. tipo de *backup*: classificação da forma como a rotina de *backup* deverá ser executada, conforme descrito nos incisos V, VI e VII do art. 5º desta Resolução;
III. frequência temporal de realização do *backup*: periodicidade na qual a rotina de *backup* deve ser executada, conforme disposto no art. 15;
IV. retenção: período em que o dado copiado no *backup* ficará retido e disponível para uso em uma eventual restauração antes de ser substituído por uma versão mais nova, definido com base no art. 16;

V. RPO (*recovery point objective*): indicador que mensura o prazo máximo de perda dados em caso de incidentes;
VI. RTO (*recovery time objective*): indicador que mensura o tempo máximo em que um sistema ou uma informação pode ficar indisponível após um incidente;
VII. janela de *backup*: período de tempo reservado para realizar a rotina de *backup*;
VIII. plano de teste de *backup* - Define a periodicidade, a abrangência, os procedimentos e as rotinas de teste que devem ser realizados; e
IX. tempo de restauração: previsão do tempo que será necessário para uma cópia ser restaurada.

§ 1º O plano de *backup* deve ser enviado via processo SEI pelo responsável técnico, com a anuência prévia e formal dos gestores das informações, para ser homologado pela DISI juntamente com o administrador de backup conforme Art 3°.

§ 2º O plano de *backup* deve 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.

§ 3º O deferimento ou indeferimento da homologação do plano de *backup* deverá ocorrer em no máximo 30 (trinta) dias após ciência da solicitação.

§ 4º O plano de *backup* homologado deverá ser implementado em até 90 (noventa) dias após a homologação.

§ 5º Os prazos que constam no § 3° e § 4° do *caput* só passarão a contar depois do encerramento dos prazos estipulados no Art. 42.

§ 6º No caso de indeferimento do plano de *backup* poderá ser enviado novo plano com os ajustes solicitados, mas os prazos contarão como se fosse uma nova solicitação.

§ 7º Os planos de *backup* homologados deverão ser armazenados em repositório digital que garanta a disponibilidade de acesso para o Superintendente da STI, o Diretor da DISI, Administrador e Operador de *backup*.

Art. 18 Os *backups* podem ser classificados como on-line, off-line ou *off-site*, a depender da forma de acesso ao *backup* realizado:
I. on-line: uma vez realizado, o *backup* é acessível dentro da rede de dados da UFMA;
II. off-line: uma vez realizado, o *backup* não é acessível em rede, sendo armazenado em mídias físicas removíveis; e
III. *off-site*: uma vez realizado, o *backup* é armazenado em outro *data center*, geograficamente separado, ou em serviço de *backup* em nuvem.

Art. 19 Os *backups* devem ter no mínimo duas cópias, realizadas em formatos de mídia distintos, sendo um on-line e outro off-line ou *off-site*.

Art. 20 Os sistemas computacionais, bases de dados e/ou repositórios de arquivos classificados como críticos devem contar, preferencialmente, com *backups* em dispositivos *off-site*.

Art. 21 A restauração de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança.

Parágrafo Único. Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de *backup.*

Seção IV
Do uso da rede

Art. 22 O administrador de *backup* deve considerar o impacto da execução das rotinas de *backup* sobre o desempenho da rede de dados da UFMA, garantindo que o tráfego necessário às suas atividades não ocasione problemas aos demais serviços de TI.

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

Art. 23 A execução do *backup* deve concentrar-se, preferencialmente, no período de janela de *backup* definido no respectivo plano de *backup*.

Parágrafo Único. 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 UFMA.

Art. 24 Deve ser observada a possibilidade de *backup*, utilizando dispositivo de armazenamento remoto, localizado em outra unidade da UFMA ou fora da UFMA (*backup* cruzado).

Seção V
Das unidades de armazenamento de backups

Art. 25 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. 26 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. 27 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. 28 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 conforme procedimentos internos.

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 VI
Dos testes de *backup*

Art. 30 Os backups devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

§ 1º Semanalmente, os *logs* de *backup* serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do *backup*.

§ 2º Ações corretivas serão tomadas quando os problemas de *backup* forem identificados, a fim de reduzir os riscos associados a *backups* com falha.

§ 3º A área técnica manterá registros de *backups* e testes de restauração para demonstrar conformidade com esta norma.

§ 4º Os testes devem ser realizados preferencialmente nos *backups* de todos os serviços críticos produzidos, independente do ambiente.

Art. 31 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.

§ 1º Os testes de restauração dos *backups* devem ser realizados por amostragem, semanalmente.

§ 2º Deve ser verificado se foi atendido os níveis de serviço pactuados no plano de *backup*, tais como o *Recovery Time Objective* (RTOs).

§ 3º Os registros de teste deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu restabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do *backup* e se o procedimento foi concluído com sucesso.

Art. 32 A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de *backup* devem ser devidamente registrados no plano de *backup*.

Seção VII
Procedimentos de restauração de backups

Art. 33 O atendimento de solicitações de restauração de dados deverá obedecer às seguintes orientações:

I. a restauração de dados deve ser solicitada via central de atendimento ao usuário da área técnica pelo gestor da informação;

II. a restauração de dados somente será considerada se houver plano de *backup* previamente aprovado e executado; e

III. 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.

Art. 34 O tempo de restauração a ser definido no plano de *backup* deve levar em consideração o tipo e o volume de dados necessários para o *restore.*

Parágrafo Único. O tempo de restauração, mencionado no *caput*, trata somente do tempo necessário para que a cópia seja restaurada, não contemplando prazos relacionados ao fluxo do processo.

Seção VIII
Do Descarte da Mídia

Art. 35 A mídia de *backup* será retirada e descartada conforme descrito nesta Resolução:

I. a área técnica garantirá que a mídia não contenha mais imagens de *backup* ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados; e

II. a área técnica garantirá a destruição física da mídia antes do descarte.

CAPÍTULO V
DAS RESPONSABILIDADES

Art. 36 O administrador de *backup* e o operador de *backup* devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de armazenamento e *backup*.

Art. 37 O administrador de *backup* deverá ser designado pelo gestor máximo da área técnica e o operador de *backup* deve ser indicado pelo administrador de *backup*.

Parágrafo Único. Caso não seja possível a indicação de pessoas distintas, uma mesma pessoa poderá exercer os papéis de administrador e operador de *backup*.

Art. 38 São atribuições do administrador de *backup*:
I. propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela UFMA;
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;
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 ao setor a que está subordinado os incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de *backups*;
IX. gerenciar mensagens e registros de auditoria (*LOGs*) de execução dos *backups*;
X. disponibilizar informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos backups;
XI. propor modificações visando ao aperfeiçoamento desta Norma de *Backup* e Restauração de Dados Digitais; e
XII. providenciar a execução dos testes de restauração.

Art. 39 São atribuições do operador de *backup*:
I. restaurar ou recuperar os *backups* em caso de necessidade;
II. operar e manusear as unidades de armazenamento de backups;
III. informar ao administrador de *backup* qualquer problema que impossibilite a criação ou restauração de um *backup*; e
IV. executar os testes de restauração de *backup*.

Art. 40 São atribuições do responsável técnico:
I. solicitar restaurações de dados, com anuência do gestor da informação;
II. sanar dúvidas técnicas do administrador de *backup* acerca das informações salvaguardadas;
III. validar, tecnicamente, o resultado das restaurações eventualmente solicitadas; e
IV. validar, tecnicamente, o resultado dos testes de restauração dos *backups*.

Art. 41 São atribuições dos gestores da informação:
I. solicitar, formalmente, a salvaguarda das informações geridas para área técnica;
II. dar anuência à solicitação feita pela área técnica para restauração de dados;
III. validar, negocialmente, o resultado das restaurações eventualmente solicitadas; e
IV. validar, negocialmente, o resultado dos testes de restauração dos backups.

CAPÍTULO VI
DAS METAS

Art. 42 A área técnica terá como metas iniciais os seguintes prazos:
I. até 3 (três) meses após a publicação desta norma para elaborar lista de ativos com classificação quanto a criticidade (críticos e não críticos);
II. até 6 (seis) meses após a publicação desta norma para elaborar 100% dos planos de *backup* dos serviços críticos de TI;
III. até 12 (doze) meses após a publicação desta norma, para providenciar a implementação de todos os planos de *backup* dos serviços críticos de TI;
IV. até 12 (doze) meses após a publicação desta norma para elaborar 100% (cem por cento) dos planos de *backup* dos serviços não críticos de TI; e
V. até 18 (dezoito) meses após a publicação desta norma para providenciar a implementação de todos os planos de *backup* dos serviços não críticos de TI.

Art. 43 A lista de ativos e os planos de *backup* deverão ser atualizados sempre que necessário e revisados, no mínimo, a cada 12 (doze) meses.

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS

Art. 44 O tratamento de dados pessoais será disciplinado em instrumento distinto pelo Plano de Implantação da Lei Geral de Proteção de Dados (LGPD).

Art. 45 Nos casos de descumprimento ou inobservância desta norma, poderão ser aplicadas sanções disciplinares na forma da Lei.

Art. 46 Esta norma poderá ser revisada a qualquer tempo, quando identificada a necessidade de alteração em qualquer de seus dispositivos.

Art. 47 Os casos omissos serão dirimidos pelo CGIT por meio da Comissão de Governança Digital e Segurança da Informação (CGDSI), que poderá expedir normas complementares, bem como disponibilizar em meio eletrônico informações adicionais.

Art. 48 Esta norma entra em vigor na data de sua publicação.

Dê-se ciência. Publique-se. Cumpra-se.

São Luís, 14 de dezembro de 2023.

FERNANDOCARVALHOSILVA148.075.133-20 Assinado de forma digital por FERNANDOCARVALHOSILVA148.075.133-20
Dados: 2023.12.21 18:23:39 -03'00'

Prof. Dr. FERNANDO CARVALHO SILVA