SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DO PARÁ
COMITÊ DE GOVERNANÇA DIGITAL DA UNIVERSIDADE FEDERAL DO PARÁ

INSTRUÇÃO NORMATIVA Nº 02/2018 - CGD, de 18 de abril de 2018.

Estabelece normas e diretrizes para auxiliar na criação, manutenção e restauração de cópias de segurança de ativos de informação em formato digital concernentes às atividades da Universidade Federal do Pará.

O Presidente do Comitê de Governança Digital da Universidade Federal do Pará, no uso das suas atribuições, que lhe confere a Portaria nº 2.111/2017 – Reitoria/UFPA, em conformidade com a Resolução de nº 727/2014, que instituiu a Política de Segurança da Informação e Comunicação da Universidade Federal do Pará, Resolução nº 693/CONSUN, de 20 de janeiro de 2011 (Regimento CTIC), com Norma Técnica ABNT NBR ISO/IEC 27001:2013, Norma Técnica ABNT NBR ISO/IEC 27002:2013, Norma Técnica ABNT NBR ISO/IEC 27005:2011 e Lei nº 12.965, de 23 de abril de 2014, resolve:

Expedir a presente **Instrução Normativa** para auxiliar na criação, manutenção e restauração de cópias de segurança dos ativos de informação da UFPA.

1. DA FINALIDADE E OBJETIVO

1.1. Esta instrução normativa tem por finalidade estabelecer normas e diretrizes para auxiliar a criação, manutenção e restauração de cópias de segurança (*backup*) de ativos de informação em formato digital, concernentes às atividades da Universidade Federal do Pará (UFPA).

2. DAS DEFINIÇÕES

2.1. Terminal: computador, *notebook*, *tablet*, *smartphone*, servidores de rede ou qualquer dispositivo com capacidade de se conectar e trocar informações através da rede da UFPA.

2.2. Aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet.

2.3. Cópia de Segurança (*backup*): cópia de segurança de ativos de informação, tais como documentos, informações administrativas e acadêmicas, dados de sistemas de informação da UFPA, entre outros.

2.4. Sistemas de Informação: *software* (programa) de computador que manipula dados e gera informações.

2.5. Dados pessoais: informações de propriedade pessoal que não tem relação com a Instituição. Dentre o rol de dados pessoais estão fotos, vídeos, documentos e qualquer outra informação digital enquadrada como não pertencente a finalidade da UFPA.

2.6. Ativos de Informação: Genericamente, informação primária compreende:

2.6.1. Informação vital para o cumprimento da missão de uma organização ou para o desempenho de seu negócio;

2.6.2. Informação de caráter pessoal, da forma em que é definida nas leis nacionais referentes à privacidade;

2.6.3. Informação estratégica necessária para o alcance dos objetivos determinados pelo direcionamento estratégico;

2.6.4. Informação de alto custo, cuja coleta, armazenamento, processamento e transmissão, demandam um longo tempo ou incorrem em um alto custo de aquisição.

2.7. Quanto à Natureza da Informação: Para compreensão didática, convém que haja uma classificação das informações quanto a sua natureza, conforme disposto a seguir:

2.7.1. Dados de sistemas de informação: banco de dados, arquivos de configuração, sítio *web*, documentação, manual de usuário, material de treinamento, procedimentos de suporte ou operação;

2.7.2. Dados administrativos: contratos, acordos, portarias, ofícios, normas e documentos afins;

2.7.3. Dados pessoais: nome, endereço, matrícula, cargo e quaisquer atributos de informação relevantes a respeito dos usuários que compõem o sistema integrado de gestão da UFPA;

2.7.4. *Logs*: dados gerados a partir de registro de eventos em sistemas de informação, na rede e nos terminais da UFPA, tais como:

2.7.4.1. Registro de conexão: conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço *IP* (*Internet Protocol*) utilizado pelo terminal para o envio e recebimento de pacotes de dados;

2.7.4.2. registro de acesso a aplicações de internet: conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço *IP*;

2.7.4.3. registro de eventos relacionados ao funcionamento de *software*: conjunto de informações que guardam data e hora de eventos de um determinado *software*;

2.7.4.3. registro de eventos relacionados ao funcionamento de ativos de rede: conjunto de informações que guardam data e hora de eventos de um ativo de rede;

2.7.4.5. registro de acesso dos usuários aos terminais: conjunto de informações referentes à data e hora de início e fim do acesso do usuário aos terminais da Instituição.

2.8. Classificação da informação

2.8.1. A informação deve ser classificada levando-se em consideração seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

2.8.2. Os proprietários de ativos de informação devem ser os responsáveis por sua classificação.

2.8.3. Os ativos de informação podem ser classificados de acordo com:

2.8.3.1. Nível de importância;

2.8.3.2. Nível de confidencialidade;

2.8.3.3. Controle de acesso.

2.9. Retenção: é o período em que os dados devem estar salvaguardados. A retenção pode variar, em ordem decrescente de prioridade, de acordo com:

2.9.1. Legislação vigente: deve levar em consideração, leis, normas, decretos e instruções normativas do governo federal;

2.9.2. Natureza e classificação da informação;

2.9.3. Proporção de dados: deve levar em consideração o volume de dados produzidos e os recursos disponíveis para *backup* e sua retenção.

2.10. Atores: São estabelecidos como atores os seguintes:

2.10.1. Proprietário da informação: pessoa ou entidade responsável pela informação, ainda que produzida por uma equipe de pessoas, sistema ou entidade externa. É a pessoa ou entidade autorizada a solicitar a recuperação do *backup* dos dados e também responsável pela validação da classificação da informação;

2.10.2. Custodiante da informação: pessoa ou entidade que zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

2.10.3. Administrador de *backup*: pessoa responsável pela criação e/ou implantação do plano de *backup*, além de ser o responsável pela administração das atividades relacionadas ao *backup*;

2.10.4. Solicitante de *backup*: pessoa que pode solicitar a restauração de dados de *backup,* ainda que não seja a proprietária dos dados, mas que seja autorizada por essa;

2.10.5. Operador de *backup*: pessoa que atua junto à equipe de administração do *backup*, realizando procedimentos relacionados às rotinas de *backup*.

2.11. Janela de *backup*: é o período definido para realização do *backup*. Deve, preferencialmente, ser realizado em horário fora do expediente de trabalho.

2.12. São estabelecidos os seguintes tipos de *backup*:

2.12.1. Completo: realiza a cópia integral dos dados;

2.12.2. Incremental: realiza a cópia das alterações ocorridas em relação ao último *backup*;

2.12.3. Diferencial: realiza a cópia, cumulativamente, das alterações ocorridas desde o último *backup* completo;

2.12.4. Pontual: realiza a cópia de informações em horário dispare. As informações contidas no *backup* Pontual podem ser completas ou de informações selecionadas.

2.13. São estabelecidos os seguintes Modos de *backup*:

2.13.1. *On-line*: ocorre sem a paralisação de atualização dos dados. O sistema provedor dos dados para *backup* continua em produção;

2.13.2. *Off-line*: ocorre com a paralisação de atualização dos dados. O sistema provedor dos dados para *backup* fica indisponível enquanto estiver ocorrendo o *backup*.

2.14. IP: "*Internet Protocol*", é um número que identifica um dispositivo em uma rede (um computador, impressora, roteador, etc).

3. DO PLANO DE *BACKUP*

3.1. O plano de *backup* estabelece os requisitos necessários para a manutenção do serviço de *backup*. O plano de *backup* deve atender, no mínimo, aos seguintes requisitos:

3.1.1. Classificação dos dados que serão salvaguardados, levando-se em consideração o nível de importância, nível de confidencialidade e controle de acesso;

3.1.2. Definição do gerente e operador(es) de *backup*;

3.1.3. Definição da janela de *backup*;

3.1.4. Definição do período de retenção do *backup*;

3.1.5. Definição do tipo (completo, diferencial e incremental) e modo (*on-line* ou *off-line*) de *backup*;

3.1.6. Definição de *softwares*, *scripts* e comandos para execução, restauração e monitoramento do *backup*;

3.1.7. Documentação sobre procedimentos de operação do serviço de *backup*, tais como agendamento do *backup*, restauração do *backup*, entre outros;

3.1.8. Definição das mídias utilizadas para *backup* de acordo com requisitos de velocidade de *backup*/restauração, escalabilidade, preservação e custos.

4. DAS DIRETRIZES PARA IMPLEMENTAÇÃO DO PLANO DE *BACKUP*

4.1. As diretrizes desta instrução normativa devem considerar, prioritariamente, os requisitos legais, os objetivos estratégicos, a estrutura e finalidade da Instituição.

4.1.1. Convém que seja dado o nível apropriado de proteção física e ambiental às informações de *backup* contidas nas mídias;

4.1.2. Convém que haja a redundância das mídias de *backup* e que elas estejam fisicamente separadas a uma distância suficiente para resguardar de danos provenientes de um desastre ocorrido no local principal de armazenamento das informações;

4.1.3. Convém que as mídias de *backup* sejam regularmente testadas para garantir que elas sejam confiáveis;

4.1.4. Convém que as cópias de *backup* sejam testadas regularmente para garantir que as ferramentas de *backup* estejam funcionando adequadamente, e que os dados salvaguardados estejam íntegros;

4.1.5. Convém que a realização do *backup* ocorra diariamente, agendada, preferencialmente, fora do horário de expediente, para não ocasionar problemas de acesso e atualização dos dados;

4.1.6. Conforme estabelecido no item 2.10.4, a solicitação de restauração de *backup* está sujeita à verificação da permissão de propriedade da informação.

4.1.7. A restauração do *backup* está sujeita à disponibilidade do dado dentro do período de retenção determinado no plano de *backup*;

4.1.8. Convém que o *backup* de dados confidenciais seja criptografado.

5. DOS ATIVOS DE INFORMAÇÃO MANDATÓRIOS PARA *BACKUP*

5.1. Compete ao Centro de Tecnologia da Informação e Comunicação – CTIC, enquanto órgão central de TIC da instituição, a salvaguarda dos seguintes dados:

5.1.1. Dados de sistemas de informação desenvolvidos, mantidos e/ou gerenciados pelo CTIC, tais como:

5.1.1.1. Sistema Integrado de Gestão da UFPA;

5.1.1.2. Sistemas legados em uso na UFPA;

5.1.1.3. Sistemas de internet, tais como: *e-mail*, servidores *web*, DNS, DHCP, VPN, etc;

5.1.1.3. Sites *web* institucionais vinculados à administração superior e hospedado nos servidores do CTIC: Portal da UFPA, CONSUN, CONSAD, CONSEPE reitoria, vice-reitoria, pró-reitoras, procuradoria, prefeitura, campi do interior e órgão suplementares.

5.1.3. *Logs*:

5.1.3.1. de sistemas de informação mantidos e gerenciados pelo CTIC;

5.1.3.2. de conexão à internet a partir de ou para os terminais da Instituição;

5.1.3.3. de acesso aos sistemas de internet gerenciadas pelo CTIC;

5.1.3.4. de ativos de rede gerenciados pelo CTIC.

6. DOS DADOS PESSOAIS DOS USUÁRIOS

6.1. A instituição não é responsável pela salvaguarda dos dados pessoais dos usuários: documentos, fotos, vídeos, etc.

6.2. É recomendado que o usuário não guarde dados pessoais nos terminais da Instituição, pois a salvaguarda de documentos ou quaisquer dados digitalizados nos equipamentos e servidores de

arquivos destina-se, prioritariamente, a manter e a proteger informações de interesse da UFPA.

6.3. A cópia de segurança (*backup)* dos arquivos pessoais, se existentes, e armazenados nos terminais institucionais é de inteira responsabilidade do usuário.

7. DO *BACKUP* DAS UNIDADES

7.1. É de responsabilidade das unidades a classificação das informações de acordo com esta instrução normativa e com a orientação do CTIC.

7.2. A classificação das informações é uma etapa que antecede o plano de *backup* e visa identificar o valor e criticidade dos dados para a Instituição.

7.3. As unidades que não dispõem de infraestrutura e pessoal para implementação do plano de *backup* devem solicitar auxílio ao CTIC, que avaliará a execução do plano de *backup* bem como a salvaguarda dos dados de acordo com a classificação da informação, recursos e pessoal disponíveis.

8. DAS CONSIDERAÇÕES FINAIS

8.1. Compete ao Comitê de Segurança da Informação (CSI) a elaboração de normas técnicas que visem atender a esta instrução normativa.

8.2. Casos omissos a esta normativa serão tratados pelo Comitê de Segurança da Informação, cabendo recurso ao Comitê de Governança Digital da Universidade Federal do Pará.

Belém, 18 de abril de 2018.

Prof. Dr. Gilmar Pereira da Silva
Presidente do Comitê de Governança Digital da Universidade Federal do Pará