I. Título

A. Nome: Instrução Normativa CITIC IN-03/2021

B. Assunto: Dispõe sobre gestão do backup e recuperação dos dados

C. Número: IN-03/2021

D. Autores: Comitê de Segurança da Informação

E. Status: [ ] proposta [ ] em revisão [X] aprovada [ ] rejeitada [ ] obsoleta

F. Quando foi proposta: 2021-06-15

G. Quando foi revisada:

H. Quando foi aprovada: 2021-11-26

I. Quando entrou em vigor: 2021-12-06

II. Definições

- **Backup:** Procedimento de cópia de segurança de dados.
- **CCUEC:** Centro de Computação da Universidade Estadual de Campinas.
- **Recuperação:** Procedimento de restauração da cópia de dados.
- ***Malware:*** Ação cibernética maliciosa.
- **Sequestro de dados:** Ataque de ação maliciosa que retém os dados que não são de propriedade do sequestrador e mediante liberação dos mesmos sob a forma de algum pagamento monetário ou não.

III. Autoridade e Responsabilidade

Os responsáveis pelos serviços e sistemas de TIC têm a responsabilidade e autoridade para gestão do backup e recuperação dos dados.

IV. Resumo

Esta política define diretrizes para toda Unicamp no que tange à gestão de backup de dados visando a continuidade de operações, a partir da guarda, proteção e recuperação dos dados.

V. Propósito

O propósito desta política é definir medidas protetivas para os dados através dos serviços de backup.

VI. Riscos do não cumprimento

A ausência de cópia de segurança de dados inviabiliza a continuidade das operações e recuperação de desastres, causando assim prejuízos financeiros ou à imagem da instituição.

VII. Escopo

A gestão do backup visa:

1. Minimizar a ameaça constante de modificação ou perda dos dados devido a exclusões acidentais, *malware* e sequestro de dados, desastres naturais ou outros eventos.

2. Permitir a restauração de um sistema ou serviço de rede a um estado confiável, livre de infecções por *malware* e que retém os dados íntegros.

VIII. Declaração da Política

É necessária a realização do backup observando o tipo de dado a ser copiado, dessa forma, os responsáveis pela criação e manutenção dos dados conjuntamente com os responsáveis pelos serviços e sistemas de TIC devem definir quais dados devem ser armazenados para backup. Para garantir a privacidade dos dados, o backup pode ser criptografado.

Como também é necessário identificar a frequência e período de retenção que estes dados devem ser armazenados de acordo com a sua classificação e criticidade. Todo ativo de informação que é imprescindível para continuidade das operações e atividades de ensino, pesquisa, extensão e administração devem ser alvo de backup.

Os Órgãos podem dispor de infraestrutura própria para a realização dos seus backups, desde que garantam que o servidor de backup esteja em uma rede exclusiva para esse fim e com acesso restrito e exclusivo aos operadores do backup. E elas também podem utilizar o serviço de backup corporativo oferecido pelo CCUEC.

Os backups deverão ocorrer em horários de menor utilização dos sistemas ou que impactem o menos possível as atividades dos Órgãos, a ser definido pelos responsáveis pelos serviços de TIC.

Deve-se realizar a simulação da restauração do backup por amostragem com periodicidade a ser definida pelo Órgão, para garantir a integridade dos dados e a capacidade de restaurar com sucesso os dados a partir do backup.

As conexões para criação do backup deverão sempre ser iniciadas pelo servidor de backup. O backup não poderá receber conexões dos clientes do serviço.

O serviço de backup não deverá permitir aos clientes a remoção de cópias, alterações, substituições ou sobrescritas das informações do backup realizado.

Independente da estratégia de backup a ser adotada, recomendamos a realização de cópias em pelo menos três locais distintos (Órgão, CCUEC e em estrutura de nuvem ou externo à Unicamp), a fim de minimizar problemas em relação à segurança e à continuidade das operações.

Os projetos de ensino e pesquisa devem pensar em formas de realizar o backup dos seus dados de forma segura e de acordo com a legislação vigente.

IX. Conformidade

A. **Verificação:** o Comitê de Segurança da Informação não tem planos de monitorar ativamente a não conformidade desta política, no entanto, irá deliberar em casos de eventos relevantes e incidentes.

B. **Notificação:**
   a. Em caso de ausência do backup, o responsável será notificado para se adequar aos critérios definidos nesta IN;
   b. Em casos omissos, a CITIC deverá ser notificada.

C. **Remediação:**
   Os responsáveis pelos serviços e sistemas de TIC, devem:
   a. Em caso de ausência do backup: redigir uma estratégia de backup considerando os critérios definidos nesta IN;
   b. Em caso de incapacidade de recuperação total ou parcial de dados, executar os seguintes passos:
   - Medir a extensão do problema nos Ativos de Informação afetados pela impossibilidade da recuperação de dados;
   - Realizar recuperação manual do dados, visando o retorno à normalidade dos serviços e sistemas de TIC;
   - Adequar-se aos critérios definidos nesta IN para confeccionar sua política de backup;
   - Reportar ao CITIC as decisões e impactos das ações realizadas.

X. Referências

1. EI-ISAC Cybersecurity Spotlight – Backups disponível em: https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-backups/.

2. Política de Backup Remoto de Máquinas Externas ao CCUEC disponível em: https://www.citic.unicamp.br/sites/default/files/normas/CITIC-IN-05-2021%20-%20regras,%20crit%C3%A9rios%20e%20procedimentos%20%20uso%20servi%C3%A7o%20de%20backup%20corporativo_1647624.pdf

Documento assinado eletronicamente por **Ricardo Dahab**, **DIRETOR GERAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**, em 19/12/2021, às 17:43 horas, conforme Art. 10 § 2º da MP 2.200/2001 e Art. 1º da Resolução GR 54/2017.

A autenticidade do documento pode ser conferida no site: sigad.unicamp.br/verifica, informando o código verificador:
73F9C61F 08B64596 A2715C77 A5FE7362

UNICAMP
SIGAD