PROTOCOLO ADMINISTRATIVO DO CENTRO DE INFORMÁTICA MÉDICA - CIMED

PRAS CIMED 001 PROTOCOLO DE CÓPIA DE SEGURANÇA E RESTAURAÇÃO DE DADOS DO HOSPITAL DAS CLÍNICAS DA FACULDADE DE MEDICINA DE BOTUCATU - HCFMB

1. OBJETIVO

Regulamentar a protocolo de backup das informações eletrônicas no âmbito do Hospital das Clínicas da Faculdade de Medicina de Botucatu (HCFMB), com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos dados sob a guarda da Gerência de Tecnologia da Informação do Centro de Informática Médica (CIMED), visando garantir a segurança, integridade e disponibilidade.

2. PÚBLICO ALVO

Equipe do Centro de Informática Médica (CIMED) responsável pela cópia de segurança e restauração de dados do HCFMB.

3. DEFINIÇÃO

Art. 1º. Para o disposto neste ato considera-se:

- **Operador de Backup:** responsável pelos procedimentos de configuração, execução e monitoramento de backup e pelo acompanhamento dos testes nos procedimentos de *restore*;
- **Backup:** cópia de segurança de dados computacionais;
- **Backup total:** backup em que todos os dados são copiados integralmente (cópia de segurança completa);
- **Backup incremental:** backup em que somente os arquivos novos ou modificados são copiados;
- **Backup diferencial:** backup em que os arquivos novos ou modificados da base de dados incremental são copiados;
- **Disaster Recovery:** estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;
- **Mídia:** meio físico no qual se armazenam os dados de um backup;
- **Retenção:** período de tempo em que o conteúdo da mídia de backup deve ser preservado;
- **Restore:** restauração de arquivos computacionais.
- **Cofre corta fogo:** Equipamento para manter a guarda das mídias magnéticas ou digitais.

3.1. Propriedade dos dados e das informações

Todo e qualquer dado ou informação (em formato lógico) gerada, adquirida, utilizada, armazenada ou que trafegue pela Rede interna de comunicação de dados é considerada propriedade exclusiva e patrimônio do Hospital das Clínicas da Faculdade de Medicina de Botucatu (HCFMB), não podendo ser interpretados como de uso pessoal, devendo ser protegida conforme estabelecido neste protocolo. Como também, todos os documentos e softwares produzidos por intermédio de seus colaboradores, durante o exercício de suas atividades profissionais, são de propriedade do HCFMB.

Toda e qualquer informação produzidas por usuários interno e usuários colaboradores, no exercício de suas funções, são patrimônio intelectual do HCFMB e não cabe a seus criadores qualquer forma de direito autoral. Quando as informações forem produzidas por terceiros para uso exclusivo do HCFMB, um instrumento próprio obrigará os criadores ao sigilo permanente do conteúdo dos produtos.

É vedada a utilização das informações a que se refere o parágrafo anterior em quaisquer outros projetos ou atividades de uso diverso ao estabelecido pelo HCFMB, salvo com autorização formal específica emitida pelo responsável pelo CIMED ou pelo Superintendente/Chefe de Gabinete. As exceções devem ser explícitas e formalizadas via memorando.

4. CONDUTA

4.1. Gestão de cópias de segurança

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que há pouco acesso de usuários ou processos automatizados aos sistemas de informática.

As mídias de backup (como LTO) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e fora do Data Center. As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de falha de gravação ou de restauração, decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas. As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de sala-cofre, em local diferente do Data Center.

Na situação de erro de backup e/ou restore é necessário que este seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, estes deverão ser autorizados apenas mediante justificativa de necessidade. Testes de restauração (restore) de backup devem ser executados pelo Operador de Backup aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup. Por se tratar de uma simulação, o executor deverá restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo Núcleo de Padronização, Auditoria e Segurança Interna. Documentos impressos não são controlados, utilize a versão armazenada eletronicamente.

4.2. Estratégia geral de backup

Art. 2°. De acordo com a natureza dos dados, trazemos a seguinte classificação:

• Servidores de Arquivos (pastas setoriais);

• Bancos de Dados (Sistema Hospitalar e afins);

• Máquinas Virtuais (imagem);

• Outros, como: Páginas WEB, Sistemas Administrativos (paralelo ao sistema MV) e Arquivos de Configuração (*The Dude, Zabbix, AD, DNS* entre outros).

Art.3°. Por padrão será adotada o seguinte esquema de realização de backups:

• *Backup Full* em mídia digital (LTO) – com retenção diária, semanal e mensal – Conforme planilha de controle de backup (utilizado e atualizado pelo Operador);

• *Backup Full* em disco do servidor – Com retenção diária.

4.3. Necessidades especiais de backup para máquinas virtuais – imagem (exceções)

Art. 4º. O backup das máquinas virtuais como imagem (adequado para fins de *disaster recovery* – ou seja: restauração da máquina como um todo), será feito apenas na seguinte periodicidade:

• *Backups* completos: a cada atualização de segurança realizada ou em caso de alterações sensíveis no sistema, a pedido do responsável pelo serviço;

• As máquinas virtuais terão o mesmo tratamento dispensado a máquinas físicas.

Art. 5º. A recuperação de backups devera obedecer às seguintes orientações:

• O usuário que necessitar recuperar arquivos deverá solicitar ao CIMED, através do sistema de chamados SOS ou Memorando, obrigatoriamente, com as informações sobre o usuário, o arquivo a ser recuperado, e a data da versão que deseja recuperar;

• Deverá ser mantido registro de todos os arquivos restaurados, acompanhado da solicitação inicial;

• Os bancos de dados serão restaurados pelo operador de backup, devendo o Núcleo de Padronização, Auditoria e Segurança Interna auxiliá-lo na tarefa de *restore*;

• Só será possível a restauração dos arquivos criados ou alterados no dia anterior a janela de realização do *backup*.

Art. 6º. Os procedimentos de backup deverão ser atualizados quando houver:

• Novas aplicações desenvolvidas ou instaladas;

• Novos locais de armazenamento de dados ou arquivos;

• Novas instalações de bancos de dados;

• Outras informações que necessitem de proteção através de *backups* deverão ser informadas ao Núcleo de Padronização, Auditoria e Segurança Interna.

Art. 7º. O descarte das mídias de *backup* inservíveis ou inutilizáveis deverá ser realizado pelo Operador de *Backup*, e com o Núcleo de Padronização, Auditoria e Segurança Interna.

Parágrafo Único: As mídias a serem descartadas deverão ser destruídas de forma a impedir a sua reutilização ou acesso indevido às informações nelas contidas por pessoas não autorizadas.

4.4. Teste de confiança

Art. 8º. Os backups mensais deverão ser testados quanto à integridade e recuperabilidade dos objetos, de maneira amostral, no prazo máximo de um mês após a sua execução.

Art. 9º. Caso seja detectada falha no *backup* ou se o mesmo estiver incompleto, um novo backup deverá ser executado com vistas ao seu armazenamento.

Art. 10º. Para todos os testes realizados deverá ser gerado um relatório que ficará sob guarda do Núcleo de Padronização Auditoria e Segurança Interna.

5. RESPONSABILIDADES

Art. 11°. O Núcleo de Padronização, Auditoria e Segurança Interna – CIMED será o administrador do backup, ficando responsável pelo protocolo, controle e procedimentos relativos aos serviços de *backup* e *restore*.

Art. 12°. São atribuições do Operador de *Backup*:

• Providenciar a criação e manutenção dos *backups*;

• Configurar a ferramenta de *backup*;

• Manter as mídias preservadas, funcionais e seguras;

• Efetuar testes de *backup* e auxiliar nos procedimentos de *restore*;

• Verificar diariamente os eventos gerados pela ferramenta de *backup*, tomando as providências necessárias para remediação de falhas;

• Restaurar os *backups* em caso de necessidade;

• Gerenciar mensagens e *logs* diários dos backups;

• Comunicar ao Núcleo de Padronização, Auditoria e Segurança Interna – CIMED os erros e as ocorrências nos *backups* e

• Propor modificações visando o aperfeiçoamento do protocolo de *backup*.

Art. 13°. Também é atribuição do Núcleo de Padronização, Auditoria e Segurança Interna:

• Dar permissão ao Operador de Backup para configurar e modificar a ferramenta cliente de *backup* no servidor;

• Validar o resultado do *restore*.

6. DISPOSIÇÕES FINAIS

Este protocolo será reavaliado a cada 2 (dois) anos ou sempre que surgirem novos requisitos tecnológicos, corporativos e/ou legais.

A implementação desse protocolo está sujeita a disponibilidade de recursos financeiros e humanos.

Este protocolo poderá ser complementado por normas e procedimentos específicos.

Casos excepcionais ou não previstos serão tratados pela Direção do CIMED e pelo Núcleo de Padronização, Auditoria e Segurança Interna.

7. RESPONSÁVEIS PELA ELABORAÇÃO E REVISÃO DO PROTOCOLO

7.1. Elaboração: Rodrigo Franco Zambom e Alexandre de O. A. Gonçalves.

7.2. Revisão: Rodrigo Franco Zambom.

8. REFERÊNCIAS

- Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais.

- Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.

9. TERMO DE AUTORIZAÇÃO DE DIVULGAÇÃO ELETRÔNICA E APROVAÇÃO DE DOCUMENTO

HOSPITAL DAS CLÍNICAS
FACULDADE DE MEDICINA DE BOTUCATU
NÚCLEO DE GESTÃO DA QUALIDADE
Av. Professor Mário Rubens Guimarães Montenegro, s/n CEP 18618-687 – Botucatu – São Paulo – Brasil
Tel. (14) 3811-6218 / (14) 3811-6215 – E-mail qualidade.hcfmb@unesp.br

TERMO DE AUTORIZAÇÃO DE DIVULGAÇÃO ELETRÔNICA E APROVAÇÃO DE DOCUMENTO

1. IDENTIFICAÇÃO DO DOCUMENTO

1.1.Título: PRAD CIMED 001 – PROTOCOLO DE CÓPIA DE SEGURANÇA E RESTAURAÇÃO DE DADOS DO HOSPITAL DAS CLÍNICAS DA FACULDADE DE MEDICINA DE BOTUCATU – HCFMB

1.2. Área Responsável: CENTRO DE INFORMÁTICA MÉDICA (CIMED)

1.3. Data da Elaboração: 15/12/2020 Total de páginas: 08 Data da Revisão: 01/09/2023

Número da Revisão: 01

1.4. Autorização de Divulgação Eletrônica do Documento e Consentimento de Exposição de dados (nome completo e número de registro profissional) durante a vigência do documento:

Eu, como autor e/ou revisor do documento citado, aprovo e autorizo a divulgação eletrônica do mesmo:

NOME	SETOR	ASSINATURA
Rodrigo Franco Zambom	CIMED	

2. DECLARAÇÃO DE CIÊNCIA, APROVAÇÃO DE DOCUMENTO E CONSENTIMENTO DE EXPOSIÇÃO DO NOME COMPLETO (DURANTE O PERÍODO DE VIGÊNCIA DO DOCUMENTO):

Declaro que estou ciente e **aprovo** o conteúdo do documento: **PRAD CIMED 001 – PROTOCOLO DE CÓPIA DE SEGURANÇA E RESTAURAÇÃO DE DADOS DO HOSPITAL DAS CLÍNICAS DA FACULDADE DE MEDICINA DE BOTUCATU – HCFMB.** Também autorizo a exposição do meu nome completo.

Data: 06/09/23	Assinatura:
	Gerente: Ricardo Aparecido Lopes