



PORTARIA Nº 316, DE 19 DE JULHO DE 2024.

Institui a nova política de *backup* e recuperação de dados digitais do Crea-MG.

O PRESIDENTE DO CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DE MINAS GERAIS - CREA-MG, no uso de suas atribuições legais e regimentais, e,

Considerando o disposto nas alíneas 'k' e 'm', do artigo 34, da Lei Federal nº 5.194, de 24 de dezembro de 1966, com suas alterações;

Considerando o disposto nos incisos V, XXVII e XLV, do artigo 96 do Regimento Interno do Crea-MG, homologado *ad referendum* pelo Plenário do Confea, através da Portaria AD nº 009, de 27 de janeiro de 2009;

Considerando a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709, de 14 de agosto de 2018), que trata sobre a proteção de dados pessoais;

Considerando a Nota Técnica GTLGPD nº 1/2019, de 19 de novembro de 2019, do Confea, que orienta os Conselhos Regionais de Engenharia e Agronomia quanto a adequação à LGPD;

Considerando a Política de Segurança da Informação (PSI), do Crea-MG, conforme portaria 265-2024;

Considerando a Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos;

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

RESOLVE:

Art. 1º Instituir a nova política de backup e recuperação dos dados digitais (PBRDD-Crea-MG), do Crea-MG.

**CAPÍTULO I
OBJETIVO E DISPOSIÇÕES GERAIS**

Art. 2º A política de backup e recuperação dos dados digitais do Conselho Regional de Engenharia e Agronomia de Minas Gerais (PBRDD – Crea-MG) é o documento que estabelece diretrizes para o processo de cópia, armazenamento dos dados e recuperação dos dados digitais sob a guarda da Divisão de Tecnologia da Informação (DTI), visando garantir a segurança, integridade e disponibilidade, em conformidade com a Política de Segurança da Informação.

Art. 3º Para os fins desta Política, considera-se:

I - Administrador de *Backup*: servidor do quadro do Crea responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de *backup* e restauração;

II - Administrador de Recurso: servidor do quadro do Crea responsável pela administração de ativo de TIC, físico ou virtual, sob responsabilidade do Conselho;

III - *Backup* Completo (full): modalidade de *backup* na qual os dados são copiados em sua totalidade;



SERVIÇO PÚBLICO FEDERAL
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DE MINAS GERAIS – CREA-MG

IV - *Backup* Diferencial: modalidade de *backup* na qual somente os arquivos novos ou modificados desde o último *backup* completo são copiados;

V - *Backup* Incremental: modalidade de *backup* na qual somente os arquivos novos ou modificados desde o último *backup* - seja ele completo, diferencial ou incremental - são copiados.

VI - Clientes de *backup*: todo equipamento servidor no qual é instalado o agente de *backup*;

VII - Recuperação de Desastre: estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;

VIII - Mídia: meio físico ou virtual no qual efetivamente armazenam-se os dados de um *backup*;

IX - Retenção: período em que o conteúdo da mídia de *backup* deve ser preservado;

X - Objeto: qualquer dado passível de *backup* e restauração;

XI - Operador de NOC: pessoa responsável por executar processos da Divisão de Tecnologia da Informação (DTI) e exercer outras atividades correlatas.

XII - Tarefa de *backup*: mecanismo que é executado sob demanda ou de acordo com um agendamento e vincula um ou mais objetos a uma modalidade de *backup* e um período de retenção.

CAPÍTULO II PADRÕES OPERACIONAIS

Art. 4º A Política de *Backup* e Recuperação de Dados Digitais deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

Art. 5º As rotinas de *backup* devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

Art. 6º 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 do Crea-MG.

CAPÍTULO III FERRAMENTAS DE BACKUP

Art. 7º As rotinas de *backup* devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

Art. 8º Os ativos envolvidos no processo de *backup* são considerados ativos críticos para o Crea-MG.

Art. 9º Compete à Divisão de Tecnologia da Informação (DTI) solicitar, à Administração, com as justificativas pertinentes, os equipamentos necessários para manter o parque de ativos sempre atualizado e em quantidade necessária ao atendimento da demanda do Crea-MG.

CAPÍTULO IV RESPONSABILIDADE E ATRIBUIÇÕES

Art. 10. São atribuições do Administrador de *Backup*:

I - Propor modificações visando o aperfeiçoamento da política de *backup*;

II - Criar e manter as tarefas de *backup*;

III - Configurar a ferramenta de *backup* e os clientes;



IV - Considerar o impacto da execução das rotinas de *backup* sobre o desempenho da rede de dados do Crea-MG;

V - Criar e manter mídias;

VI - Testar o *backup* e a restauração;

VII - Criar notificações e relatórios;

VIII - Verificar periodicamente os relatórios gerados pela ferramenta de *backup*;

IX - Restaurar os *backups* em caso de necessidade;

X - Gerenciar mensagens e logs diários dos *backups*, fazendo o tratamento dos erros de forma que o procedimento de *backup* tenha sequência e os erros na sua execução sejam eliminados;

XI - Fazer manutenções periódicas dos dispositivos de *backup*;

XII - Fazer o carregamento das mídias necessárias para os *backups* programados.

Art. 11. Os procedimentos de *backup* deverão ser atualizados quando houver:

I - Novas aplicações desenvolvidas;

II - Novos locais de armazenamento de dados ou arquivos;

III - Novas instalações de bancos de dados;

IV - Novos aplicativos instalados;

V - Outras informações que necessitem de proteção através de *backups* deverão ser informadas ao Administrador de *Backup*, pelo Administrador de Recurso.

Art. 12. A retenção dos *backups* deve observar os seguintes prazos:

I - Diário: retenção em storage NAS de 7 dias, trata-se de file system;

II - Semanal: retenção em disco por 15 dias, trata-se de máquinas virtuais;

III - File Server: retenção de 3 meses.

Parágrafo único: Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada ou destruída, observando sempre seu estado de utilização e número de leitura/gravação.

CAPÍTULO V DAS OBRIGAÇÕES GERAIS

Art. 13. A criação e a operação dos *backups* deverão obedecer às seguintes orientações:

I - Criação de *backups*:

a) O *backup* deverá ser programado para execução automática em horários de menor utilização dos sistemas;

b) O *backup*, preferencialmente, deverá ser realizado através da rede de *backup*.

II - Operação de *backups*:

a) O *backup* deverá ser monitorado pelo Operador NOC;

b) Para todos os *backups* realizados, deve ser gerado um extrato automatizado pela própria ferramenta de *backup*. Tal extrato deverá ser enviado por e-mail para o Administrador de *Backup*;

c) O Operador de NOC deverá gerar, por amostragem, relatório geral, mensal da execução de tais *backups*.



SERVIÇO PÚBLICO FEDERAL
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DE MINAS GERAIS – CREA-MG

Art. 14. Os *backups* deverão ser realizados, preferencialmente, como disposto a seguir:

I - Os *backups* diários serão executados de segunda à sexta-feira, às 19h, em modo incremental;

II - Os *backups* semanais serão executados nos finais de semana, iniciando aos sábados, em modo full (completo);

III - Em caso de falha em algum procedimento de *backup* ou impossibilidade da sua execução, o Administrador de *Backup* deverá adotar as providências necessárias para promover a salvaguarda das informações através de outro mecanismo, como por exemplo: nova execução do backup em horário de comercial ou cópia dos dados para outro servidor.

Art. 15. A recuperação de *backups* deverá obedecer às seguintes orientações:

I - A solicitação de recuperação de objetos deverá, sempre, iniciar-se com o responsável pelo recurso, através de chamado técnico, utilizando a ferramenta de controle de atendimentos do Crea-MG, GLPI;

II - O chamado técnico deve conter, ao menos, o nome e setor do usuário, o(s) objeto(s) a ser(em) recuperado(s), localização em que se encontra(m), a data da versão que deseja recuperar, local alternativo para o armazenamento do(s) objeto(s) recuperado(s), se for o caso, e a justificativa para recuperação;

III - Este chamado será encaminhado ao Administrador de *Backup*, que após a conclusão da tarefa, realizará o fechamento do chamado indicando a restauração do(s) objeto(s).

IV - A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de *backup*.

CAPÍTULO VI DISPOSIÇÕES FINAIS

Art. 16. Esta política será reavaliada a cada 2 (dois) anos ou sempre que surgirem novos requisitos tecnológicos, corporativos e/ou legais.

Art. 17. A implementação dessa política está sujeita a disponibilidade de recursos financeiros e humanos. Esta política poderá ser complementada por normas e procedimentos específicos.

Art. 18. Casos excepcionais ou não previstos serão tratados pela Divisão Tecnologia da Informação.

Art. 19. Esta Política não exclui as demais normas de segurança da informação aprovadas pelo Comitê de Resposta a Incidentes do Crea-MG e demais normas do Conselho referentes a privacidade e proteção de dados pessoais.

Art. 20. O uso inadequado do disposto nesta Portaria fica sujeito à apuração de responsabilidade penal, civil e administrativa, na forma da legislação em vigor.

Art. 21. Esta Portaria entra em vigor na data de sua assinatura.

Art. 22. Revogam-se as disposições em contrário.

Art. 23. Dê-se ciência e cumpra-se.

Belo Horizonte, 19 de julho de 2024.

Eng. Civil e de Seg. do Trabalho Marcos Venícius Gervásio
Presidente do Crea-MG