tecnologia a serviço da cidade
procempa

Política de Cópias de Segurança

Julho, 2022

Cópias de Segurança ou Backup

1. Cada usuário é responsável pela manutenção de cópias de segurança dos arquivos de dados em suas estações de trabalho ou notebooks.
2. Arquivos tratados nas estações de trabalho ou notebooks que necessitem cópia de segurança deverão ser armazenados em servidor de arquivos apropriado da companhia, conforme autorizado pelo supervisor. Deve ser solicitada confirmação da Equipe de Backups de que os sistemas de arquivos usados estão includidos nas cópias de segurança.
3. Não é permitida a cópia de dados confidenciais para tratamento, processamento ou armazenamento em serviços externos, ou equipamentos de terceiros não contratados formalmente pela companhia ou cliente para tal finalidade.
4. Sempre que possível, os dados confidenciais devem estar criptografados nos backups.
5. Rotinas de backup das bases de dados, servidores e sistemas devem seguir padrão existente. Exceções a estes procedimentos devem ser informadas pelo responsável do sistema.
6. O responsável pelo servidor deverá solicitar processo de backup das informações necessárias para recuperação dos serviços, incluindo banco de dados e aplicações, conforme plano de continuidade de negócio e recuperação de desastre.
7. Todo o backup deve ser verificado periodicamente quanto à funcionalidade e possibilidade de recuperação pelo responsável do sistema.
8. Mídias de armazenamento devem ser mantidos em local seguro e devem ser respeitados os parâmetros de vida útil sugeridos pelo fabricante das mesmas.
9. Deve ser respeitado o tempo de retenção de informação definido pela legislação e normas pertinentes, inclusive LGPD e Marco Civil da Internet. Além das mídias de backup, a Equipe de Backups deve estar atenta para manter operacionais os equipamentos necessários para recuperação dos dados quando necessário durante o período de retenção.