POLÍTICA

DE

BACKUP

NR Nº 004/2020 – POLÍTICA DE BACKUP

1. INTRODUÇÃO

Backup é um processo de cópia de segurança de uma informação para outro dispositivo de armazenagem (fita, disco remoto, etc.), pois caso ocorra algum acidente eventual com a informação original, existe a possibilidade de se retornar os dados de maneira rápida e segura. Os aplicativos nas empresas podem gerar grandes quantidades de informações e a cópia e guarda de uma quantidade significativa dessas informações é fundamental para a segurança das informações em uma empresa.

Normalmente o backup (também conhecido como cópia de segurança ou reserva) é uma tarefa administrativa de responsabilidade do administrador do sistema. Uma boa arquitetura de backup e recuperação deve incluir um plano de prevenção de desastres, procedimentos e ferramentas que ajudem na recuperação de um desastre ou falha de energia, além de procedimentos e padrões para realizar a recuperação.

O Recovery (recuperação) é a recuperação dos arquivos. Ao fazer um backup dispomos de uma cópia dos dados em outro local, seja ele físico ou virtual. Através do recovery os dados são recuperados e repostos nos servidores no formato anterior ao problema ou do erro fatal ocorrido no processamento.

Nenhuma estratégia de backup atende a todos os sistemas. Uma estratégia que é adequada para um sistema poderá ser imprópria para outro sistema. O administrador deve determinar com precisão a estratégia que melhor se adequar a cada situação.

O Instituto Conab de Seguridade Social - CIBRIUS, buscando preservar a integridade de seus dados e informações arquivadas em meios eletrônicos, quer com este trabalho estabelecer diretrizes e procedimentos técnicos e operacionais, facilitando a guarda, a recuperação e o acesso aos seus dados e informações tão imprescindíveis para o seu funcionamento.

2. DO OBJETIVOS

2.1. Orientar/estabelecer procedimentos visando manter a integridade e disponibilidade dos dados, das informações e dos recursos de processamento de informação do CIBRIUS, evitar a interrupção das atividades de negócio, preservar os dados e informações armazenadas eletronicamente, proteger os processos críticos contra defeitos, falhas ou desastres significativos, assegurar a sua retomada em tempo hábil e definir procedimento de cópias de segurança dos dados e informações de propriedade do CIBRIUS.

3. DA APLICAÇÃO

3.1. Diretrizes de implementação

3.1.1. Garantir que os dados e as informações possam ser recuperados após falha técnica, elétrica, ou desastre, utilizando padrões de armazenamento e recuperação dos dados e informações inerentes às atividades do CIBRIUS.

3.1.2. Garantir o atendimento à Legislação vigente.

3.1.3. Definir um plano de prevenção de desastres, procedimentos operacionais e, principalmente, ferramentas e equipamentos que ajudem na geração de cópias de segurança garantindo a recuperação de dados e informações no menor intervalo de tempo, é a principal diretriz deste trabalho, evitando assim a interrupção das atividades do Instituto. Neste contexto serão implementadas através do Plano de *Backup* do CIBRIUS as seguintes ações:

3.1.3.1. Definição do nível necessário das cópias de segurança das informações;

3.1.3.2. Produção de registros e extratos das cópias de segurança e documentação apropriada sobre os procedimentos de restauração da informação;

3.1.3.3. Testes regulares em mídias de cópia de segurança para garantir que elas são suficientemente confiáveis em uso emergencial, quando necessário;

3.1.3.4. Testes regulares dos Procedimentos de Recuperação de dados e informações, de forma a garantir que esses são efetivos e que podem ser concluídos dentro dos prazos definidos; e

3.1.3.5. Frequência das cópias de segurança.

4. DAS CONCEITUAÇÕES

4.1. Backup: cópia de segurança de arquivos de dados, informações e configurações de hardware e software mantida para permitir a recuperação dos dados originais em caso de falha ou indisponibilidade do sistema.

4.2. Sistema: sistema de acesso dos usuários à rede interna do Cibrius e aos demais sistemas.

4.3. Dado: registro ou fato em sua forma primária, usado para representar uma quantidade, um objeto etc.

4.4. Informação: resultado da organização ou combinação de dados de forma significativa e contextual.

4.5. Patch: correção temporária de problemas detectados em código de software, liberada antes da conclusão de uma correção definitiva a ser ofertada na próxima versão do programa.

4.6. Credenciais: informações específicas e de responsabilidade de cada usuário para acesso a sistemas/informações do Cibrius.

4.7. Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável ou qualquer informação que identifique ou possa identificar uma pessoa física, tais como nomes, números, códigos de identificação, endereços, imagens (fotos).

4.8. Dados pessoais sensíveis: informações sobre origem racial ou étnica, convicção religiosa, opinião pública, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou vida sexual, dado genético ou biométrico quando vinculado à uma pessoa natural.

4.9. Tratamento de dados: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

4.10. Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada

4.11. Segurança da informação: processo de preservar a informação levando em conta os seguintes objetivos:

4.11.1. Confidencialidade: garantia de que o acesso à informação é restrito aos seus usuários legítimos;

4.11.2. Integridade: garantia da informação livre de erro e da proteção contra sua adulteração; e

4.11.3. Disponibilidade: garantia de que as informações estejam disponíveis para os usuários legítimos de forma oportuna.

4.12. Sistema: conjunto de elementos ou componentes que interagem para produzir resultados previamente definidos. Os sistemas são compostos de entradas, saídas e mecanismos de processamento e feedback ou retroalimentação.

4.13. Usuário: funcionário, gerente, dirigente, membro de conselho, prestador de serviços, estagiário, representante de fornecedor ou qualquer outro indivíduo que concorra para a realização do trabalho no Cibrius, ao qual tenha sido concedido acesso aos recursos de informação e tecnologia do Instituto.

5. DOS CRITÉRIOS E PROCEDIMENTOS

5.1. Armazenamentos de Dados.

5.1.1. Todos os documentos, banco de dados e informações eletrônicas relevantes e relacionadas ao CIBRIUS devem ser armazenados de forma centralizada, em servidor próprio;

5.1.2. Após o armazenamento local, os backups, devem ser enviados para um diretório remoto onde permanecerão(retenção) pelo tempo estipulado e definido no quadro a seguir.

5.1.3. Para a realização dos backups, as informações sobre os servidores, o local de guarda/armazenamento, os dias e horários que serão executados, além do tempo de retenção, serão definidos e formalizados pela Área de Informática, com a

ciência do Diretor hierárquico responsável, permanecendo disponíveis para consulta na rede do Cibrius.

Observação 1: Os prazos de retenção de informações observarão a Legislação vigente.
Observação 2: O detalhamento operacional para a realização do backup, que trata o item "5.1.3" será atualizado e registrado no arquivo "Servidor\corporativa\informática\Documentos\Política de backup e controles\Plano de Backup", em substituição de informações deste item, quando necessário:

5.2. Rotinas de Backup Diário

5.2.1. O *backup* deve ser realizado todos os dias, nos horários definidos conforme Plano de Backup.

5.3. Rotinas de Backup Mensal

5.3.1. O processo de backup mensal deve ser realizado no último dia útil de cada mês, nos horários definidos conforme Plano de Backup.

5.4. Rotinas de Backup Anual

5.4.1. O processo de backup anual deve ser realizado na última sexta-feira do ano, nos horários definidos conforme Plano de Backup.

5.5. Armazenamento

5.5.1. Todas as cópias de dados e informações (backup) do CIBRIUS deverão ser gravadas em disco e terão a seguinte destinação:

5.5.1.1. Backup Diário - deve ser realizado e enviado diretamente para um diretório remoto (nuvem) e lá ficará retido por 7 dias, conforme definição por parte da Área de Informática.

5.5.1.2. Backup Mensal - deve ser realizado e enviado diretamente para um diretório remoto (nuvem) e lá ficará retido por 12 meses, conforme definição por parte da Área de Informática.

5.5.1.3. Backup Anual - deve ser realizado e enviado diretamente para um diretório remoto (nuvem) e lá ficará retido por 5 anos, conforme definição por parte da Área de Informática.

5.6. Responsáveis pelo processo de backup e suas atribuições:

5.6.1. Cabe à Área de Informática a responsabilidade sobre o processo de cópia ou backup dos dados e informações eletrônicas do Cibrius, e dentre outras atribuições:

- Cumprir e fazer cumprir todos os procedimentos e recomendações do Plano de *Backup* do CIBRIUS;
- Realizar o *backup* diário, mensal e anual;
- Preparar os equipamentos de segurança para a guarda local e externa, preservando a integridade dos dados e informações;
- Realizar todas as tarefas provenientes do processo de *backup* e do Plano de *backup* do CIBRIUS; e

- Orientar os usuários para o adequado uso dos dados e informações, evitando o armazenamento de dados desnecessários, bem como a restauração de informações consideradas descartáveis.

5.7. Restauração de Backups

5.7.1. Periodicidade e Responsabilidade

5.7.1.1. A restauração dos *backup*s, a título de teste, será realizada a cada 90 (noventa) dias.

5.7.2. Controle

5.7.2.1. As solicitações de restauração serão realizadas por escrito ou através de mensagem eletrônica.

5.7.3. Acesso

5.7.3.1. As credenciais para acesso ao portal onde se encontram os backups estão no arquivo:

- Servidor\corporativa\informática\Documentos\Política de backup e controles\plano de backup

6. DA COMPETÊNCIA

6.1. À Diretoria Executiva do Cibrius:

6.1.1. Aprovar as normas operacionais oriundas das diretrizes de segurança registradas nesta Política de Segurança da Informação, a serem elaborada pela área responsável por sua implementação; e

6.1.2. Prover os recursos necessários para o desenvolvimento das ações de segurança a cargo da ÁREA DE INFORMÁTICA e demais unidades executoras.

7. DISPOSIÇÕES GERAIS

7.1. Esta Política está baseada também, nas melhores práticas do setor aplicadas ao assunto que se refere.

7.2. Os casos omissos serão analisados e decididos pela Diretoria Executiva.

8. DA VIGÊNCIA

8.1. Esta norma entra em vigor a partir da data de sua aprovação pelo Conselho Deliberativo.

APROVADA

11ª Reunião Ordinária do Conselho Deliberativo - Exercício 2020.

EM: 16/12/2020