

Sugestões de Segurança do Banco de Dados

Em primeiro lugar reforçamos que a **DAPE SOFTWARE** não é responsável pelos Recursos de Processamento de Dados do Cliente tais como Banco de Dados, Servidores, Equipamentos e Infraestrutura de Rede, até porque os mesmos normalmente são utilizados em outras aplicações dentro da empresa ou escritório contábil, o que não nos impede de prestar serviços pontuais relacionados e específicos aos sistemas da **DAPE SOFTWARE** quando combinado entre ambos.

A importância do Backup do Banco de Dados

O Banco de Dados **Pegasus10** é o local onde está armazenado todas as informações referentes aos sistemas Folha de Pagamento e eSocial da sua empresa, por isso a importância de se fazer **Backup** Diário do seu Banco de Dados.

Fazer **Backup** constantemente é de suma importância para proteger seus dados contra o risco de perda, seja por problemas em equipamentos, pessoa má intencionada, sequestro de informações, entre tantas outras possibilidades que podem ocorrer, por isso resolvemos descrever algumas boas práticas na segurança dos seus dados.

Backup Automático

O **Backup** manual sempre oferece mais riscos, pois está sujeito a falhas humanas diversas, como esquecimento, armazenamento indevido ou até mesmo conhecimento técnico insuficiente. Além disso, toma muito tempo e reduz a produtividade operacional.

Por isso, as melhores práticas recomendam automatizar o **Backup**, de modo que ocorram de forma recorrente, respeitando as especificidades e regras do seu negócio.

Podemos efetuar automatização do **Backup** da Base de Dados **Pegasus10** a fim de melhorar a segurança dos dados. O Backup pode ser agendado para fazer automaticamente todos os dias no diretório padrão de Backup.

Caso necessário podemos lhe auxiliar nesse processo, para isso entre em contato com o nosso suporte, teremos o maior prazer em lhe auxiliar.

A **DAPE SOFTWARE** não é responsável pela segurança do banco de dados da sua empresa e nem pela manutenção dos seus **Backups**, portando chamamos a atenção para que adote medidas e procedimentos a fim de manter suas informações em segurança.

Boas Práticas para segurança

- Monitoramento dos Recursos (Espaço em Disco, Memória Utilizada, Estrutura de Rede, ...);
 - Verificação dos Eventos do Sistema Operacional e de Banco de Dados a fim de verificar se não estão ocorrendo erros;
 - Verificação se está sendo efetuado corretamente os **Backups** conforme as regras estabelecidas;
 - Verificar a integridade dos **Backups**.
 - Copiar o arquivo de **Backup** para pelo menos um outro local seguro, fora do Servidor onde está instalado o Banco de Dados (Obs. de preferência datar o nome do **Backup** a fim de poder manter vários dias de **Backup**), protegendo desta forma as cópias de um possível acesso externo;
 - Verificar a integridade da cópia que foi feita no item anterior;
 - Assegurar que a cópia do arquivo de **Backup** esteja segura de um possível sequestro de informações.
- Essas são algumas poucas sugestões para se manter a segurança das informações.

Colocamo-nos a disposição para quaisquer esclarecimentos.

Equipe DAPE SOFTWARE / PEGASUS