

Sistema de Backup - Dados dos Clientes

IMPORTANTE: GitHub vs Banco de Dados

O que vai para o GitHub:

- Código-fonte** (frontend, backend, APIs)
- Configurações** (package.json, tsconfig, etc)
- Documentação** (README, guias)
- Scripts** (automação, deploy)

O que NÃO vai para o GitHub:

- Dados dos clientes** (nome, telefone, email)
- Agendamentos** (horários, serviços)
- Vendas** (transações financeiras)
- Produtos** (estoque, movimentações)
- Senhas** (credenciais, tokens)

Por quê? Segurança, LGPD e privacidade dos seus clientes!

Sistema de Backup Completo

1 Backup Automático Diário (RECOMENDADO)

Este sistema faz backup do banco de dados todos os dias às 3h da manhã automaticamente:

```
cd /home/ubuntu/sistema_salao_beleza
chmod +x scripts/backup-auto.sh
chmod +x scripts/setup-cron.sh

# Configurar backup automático diário
bash scripts/setup-cron.sh
```

Localização dos backups:

- Diretório: /home/ubuntu/backups/database/
- Formato: auto_backup_YYYYMMDD_HHMMSS.backup
- Retenção: 30 dias (backups antigos são apagados automaticamente)

2 Backup Manual (Quando Quiser)

Para fazer backup imediatamente:

```
cd /home/ubuntu/sistema_salao_beleza/nextjs_space
yarn tsx scripts/backup-database.ts
```

O que é salvo no backup:

- Todos os salões cadastrados
- Todos os usuários e senhas

- Todos os clientes
 - Todos os profissionais
 - Todos os serviços e produtos
 - Todos os agendamentos (passados e futuros)
 - Todas as vendas e pagamentos
 - Todo o estoque e movimentações
 - Todas as configurações
 - Arquivo .env com as credenciais
-



Onde Ficam os Backups

Local Seguro no Servidor

```
/home/ubuntu/backups/
└── database/
    ├── auto_backup_20251106_030000.backup
    ├── auto_backup_20251105_030000.backup
    └── backup_2025-11-06T10-30-00.json.gz
└── env/
    ├── .env_20251106_030000
    └── .env_20251105_030000
└── logs/
    ├── auto_backup_20251106_030000.log
    └── auto_backup_20251105_030000.log
```



Backup em Nuvem (EXTRA SEGURANÇA)

Opção 1: Google Drive (Recomendado para iniciantes)

1. Instalar rclone:

```
curl https://rclone.org/install.sh | sudo bash
```

1. Configurar Google Drive:

```
rclone config
```

- Escolha: `n` (New remote)
- Nome: `gdrive`
- Storage: `drive` (Google Drive)
- Siga as instruções para autorizar

1. Script de Upload Automático:

```
# Criar script de upload
cat > /home/ubuntu/sistema_salao_beleza/scripts/backup-to-gdrive.sh << 'EOF'
#!/bin/bash
BACKUP_DIR="/home/ubuntu/backups"
DATE=$(date +%Y%m%d)

# Upload para Google Drive
rclone sync "$BACKUP_DIR" gdrive:SistemaBelez/backups \
--log-file="/home/ubuntu/backups/logs/gdrive_$DATE.log" \
--log-level INFO

echo "✓ Backup enviado para Google Drive: $DATE"
EOF

chmod +x /home/ubuntu/sistema_salao_beleza/scripts/backup-to-gdrive.sh
```

1. Automatizar Upload Diário:

```
crontab -e
```

Adicione:

```
0 4 * * * /home/ubuntu/sistema_salao_beleza/scripts/backup-to-gdrive.sh
```

Opção 2: Dropbox

```
# Instalar Dropbox Uploader
curl "https://raw.githubusercontent.com/andrefabrizi/Dropbox-Uploader/master/dropbox_uploader.sh" -o ~/dropbox_uploader.sh
chmod +x ~/dropbox_uploader.sh
~/dropbox_uploader.sh

# Seguir instruções para autorizar
```

Opção 3: AWS S3 (Já configurado no sistema)

O sistema já usa AWS S3 para fotos. Podemos usar para backups também:

```
# Instalar AWS CLI
sudo apt-get update
sudo apt-get install awscli -y

# Configurar (usar as mesmas credenciais do .env)
aws configure
```



Sistema de Alertas

Receber email quando backup falhar:

1. Instalar sendmail:

```
sudo apt-get install sendmail -y
```

1. Editar script de backup:

```
nano /home/ubuntu/sistema_salao_beleza/scripts/backup-auto.sh
```

Descomentar linha:

```
echo "Backup falhou em $(date)" | mail -s "ALERTA: Backup Falhou" sistem-
abeleza.contato@gmail.com
```

Como Restaurar um Backup

Se algo der errado, você pode restaurar tudo:

```
cd /home/ubuntu/sistema_salao_beleza
bash scripts/restore.sh
```

Ele vai:

1. Listar todos os backups disponíveis
2. Você escolhe qual restaurar
3. Sistema volta ao estado daquele backup

Checklist de Segurança

- [] Backup automático diário configurado
- [] Backups sendo enviados para nuvem (Google Drive/Dropbox)
- [] Testei restaurar um backup (para garantir que funciona)
- [] Sistema de alertas configurado
- [] Mantendo pelo menos 30 dias de backups
- [] Tenho backups em 2 locais diferentes (servidor + nuvem)
- [] Verifico os logs semanalmente

Plano de Backup Recomendado

Nível Básico (MÍNIMO):

-  Backup automático diário local
-  Retenção de 30 dias

Nível Intermediário (RECOMENDADO):

-  Backup automático diário local
-  Upload semanal para Google Drive

- Retenção de 90 dias

Nível Profissional (IDEAL):

- Backup automático diário local
 - Upload diário para Google Drive
 - Upload semanal para segundo serviço (Dropbox/AWS)
 - Retenção de 180 dias
 - Sistema de alertas por email
 - Teste de restauração mensal
-



Estatísticas

Tamanho aproximado dos backups:

- 10 clientes: ~2-5 MB
- 100 clientes: ~10-20 MB
- 1000 clientes: ~50-100 MB

Frequência recomendada:

- Uso leve (1-10 agendamentos/dia): Backup diário
 - Uso moderado (10-50 agendamentos/dia): Backup diário + semanal para nuvem
 - Uso intenso (50+ agendamentos/dia): Backup diário + diário para nuvem
-



Comandos Úteis

Ver últimos backups:

```
ls -lh /home/ubuntu/backups/database/ | tail -10
```

Ver espaço usado:

```
du -sh /home/ubuntu/backups/
```

Ver logs de backup:

```
cat /home/ubuntu/backups/logs/auto_backup_$(date +%Y%m%d)*.log
```

Testar se backup está funcionando:

```
cd /home/ubuntu/sistema_salao_beleza/nextjs_space
yarn tsx scripts/backup-database.ts
```



Dicas Importantes

1. **Teste a restauração:** Faça um teste de restauração pelo menos 1 vez por mês
2. **Múltiplas cópias:** Sempre tenha backups em pelo menos 2 locais diferentes
3. **Monitore regularmente:** Verifique os logs de backup toda semana
4. **Proteja o .env:** O arquivo .env tem todas as senhas, mantenha-o seguro
5. **LGPD:** Os backups contêm dados pessoais, mantenha-os seguros



Segurança dos Backups

Os backups estão protegidos:

- Armazenados em diretório com permissões restritas
- Arquivo .env tem permissão 600 (só você pode ler)
- Backups são comprimidos (.gz) para economizar espaço
- Backups antigos são apagados automaticamente
- Senhas do banco NÃO vão para o GitHub

Para aumentar segurança:

```
# Criptografar backups antes de enviar para nuvem
gpg --symmetric --cipher-algo AES256 backup_file.backup
```



Suporte

Se tiver dúvidas, consulte:

- `BACKUP_GUIA_COMPLETO.md` - Guia técnico detalhado
- `GUIA_RAPIDO_BACKUP.md` - Comandos rápidos
- Logs em: `/home/ubuntu/backups/logs/`

LEMBRE-SE: Código vai para GitHub, Dados ficam em Backups!