🚀 Guia de Deploy - Vision Estoque Financeiro

✅ Status das Correções de Segurança

Todas as **9 vulnerabilidades críticas** foram corrigidas e implementadas:

1. ✅ **Debug Mode Desabilitado** - Configurado via ambiente
2. ✅ **Validação de Uploads** - MIME types, magic numbers, tamanho
3. ✅ **Sistema de Autenticação** - Token opcional implementado
4. ✅ **Dados Sensíveis Protegidos** - Logs sanitizados
5. ✅ **Binding Seguro** - Configuração por ambiente
6. ✅ **Headers de Segurança** - Flask-Talisman configurado
7. ✅ **Rate Limiting** - 10 uploads/minuto por IP
8. ✅ **CORS Configurado** - Origens permitidas definidas
9. ✅ **Sanitização de Prompts** - Proteção contra injeção

🛠️ Pré-requisitos

1. **Google Cloud Account** com projeto criado
2. **gcloud CLI** instalado e configurado
3. **Permissões necessárias**:
   - Cloud Run Admin
   - Artifact Registry Admin
   - Cloud Build Editor
   - Storage Admin

📋 Passos para Deploy

1. Autenticação no Google Cloud

```
# Fazer login
gcloud auth login

# Configurar projeto (substitua pelo seu PROJECT_ID)
gcloud config set project vision-estoque-financeiro
```

2. Configurar Variáveis de Ambiente

Edite o arquivo `.env.production` com suas configurações:

```
cp .env.production .env
# Edite o arquivo .env com suas configurações reais
```

⚠️ **IMPORTANTE**: Altere os seguintes valores:
- `SECRET_KEY`: Gere uma chave segura
- `GCP_PROJECT_ID`: Seu ID do projeto Google Cloud

- `GCS_BUCKET_NAME`: Nome do bucket para uploads
- `API_TOKEN`: Token seguro se habilitar autenticação

3. Executar Deploy Automatizado

```
# Executar script de deploy
./deploy.sh
```

O script irá:
- ✅ Verificar autenticação
- ✅ Habilitar APIs necessárias
- ✅ Criar repositório no Artifact Registry
- ✅ Fazer build da imagem
- ✅ Deploy no Cloud Run
- ✅ Testar endpoint de saúde

4. Deploy Manual (Alternativo)

Se preferir fazer o deploy manualmente:

```
# Definir variáveis
PROJECT_ID="seu-project-id"
REGION="us-central1"
SERVICE_NAME="vision-estoque"
IMAGE_NAME="vision-estoque"
TAG="v$(date +%Y%m%d-%H%M%S)"

# Habilitar APIs
gcloud services enable cloudbuild.googleapis.com run.googleapis.com artifactre-
gistry.googleapis.com

# Criar repositório
gcloud artifacts repositories create cloud-run-source-deploy \
    --repository-format=docker \
    --location=${REGION}

# Build da imagem
gcloud builds submit --tag ${REGION}-docker.pkg.dev/${PROJECT_ID}/cloud-run-source-de-
ploy/${IMAGE_NAME}:${TAG}

# Deploy no Cloud Run
gcloud run deploy ${SERVICE_NAME} \
    --image ${REGION}-docker.pkg.dev/${PROJECT_ID}/cloud-run-source-deploy/${IM-
AGE_NAME}:${TAG} \
    --region ${REGION} \
    --platform managed \
    --allow-unauthenticated \
    --port 8080 \
    --memory 1Gi \
    --set-env-vars "FLASK_ENV=production,GCP_PROJECT_ID=${PROJECT_ID}"
```

🔧 Configurações Pós-Deploy

1. Configurar Bucket GCS

```
# Criar bucket para uploads
gsutil mb gs://vision-estoque-financeiro-uploads

# Configurar CORS
echo '[{"origin": ["*"], "method": ["GET", "POST"], "responseHeader": ["Content-
Type"], "maxAgeSeconds": 3600}]' > cors.json
gsutil cors set cors.json gs://vision-estoque-financeiro-uploads
```

2. Configurar Secret Manager (Recomendado)

```
# Criar secrets
echo "your-super-secret-key" | gcloud secrets create flask-secret-key --data-file=-
echo "your-api-token" | gcloud secrets create api-token --data-file=-

# Atualizar Cloud Run para usar secrets
gcloud run services update vision-estoque \
    --update-secrets SECRET_KEY=flask-secret-key:latest \
    --update-secrets API_TOKEN=api-token:latest \
    --region us-central1
```

3. Configurar Domínio Customizado (Opcional)

```
# Mapear domínio
gcloud run domain-mappings create \
    --service vision-estoque \
    --domain yourdomain.com \
    --region us-central1
```

🔍 Verificação e Testes

Endpoints Disponíveis

- **Health Check**: `GET /health`
- **Upload de Nota**: `POST /upload-invoice`
- **Página Principal**: `GET /`

Teste de Funcionalidade

```
# Obter URL do serviço
SERVICE_URL=$(gcloud run services describe vision-estoque --region=us-central1 --
format="value(status.url)")

# Testar health check
curl "${SERVICE_URL}/health"

# Testar upload (com arquivo)
curl -X POST -F "image=@test-invoice.jpg" "${SERVICE_URL}/upload-invoice"
```

📊 Monitoramento

Visualizar Logs

```
# Logs em tempo real
gcloud run logs tail vision-estoque --region=us-central1

# Logs específicos
gcloud run logs read vision-estoque --region=us-central1 --limit=50
```

Métricas no Console

Acesse: https://console.cloud.google.com/run/detail/us-central1/vision-estoque

🔐 Configurações de Segurança

Habilitar Autenticação

1. Edite `.env` ou configure via Cloud Run:

```
ENABLE_AUTH=true
API_TOKEN=seu-token-super-seguro
```

1. Use o token nas requisições:

```
curl -H "Authorization: Bearer seu-token-super-seguro" "${SERVICE_URL}/upload-invoice"
```

Headers de Segurança Implementados

- ✅ Content Security Policy (CSP)
- ✅ X-Frame-Options: SAMEORIGIN
- ✅ X-Content-Type-Options: nosniff
- ✅ Referrer-Policy: strict-origin-when-cross-origin
- ✅ Permissions-Policy

Rate Limiting

- ✅ 10 uploads por minuto por IP
- ✅ Configurável via variáveis de ambiente

🚨 Troubleshooting

Problemas Comuns

1. **Erro de Autenticação**
   `bash`
   `gcloud auth login`
   `gcloud config set project SEU_PROJECT_ID`

2. **Erro de Permissões**
   - Verifique se tem as roles necessárias
   - Execute: `gcloud projects get-iam-policy SEU_PROJECT_ID`

3. **Erro de Build**
   - Verifique se o Dockerfile está correto
   - Verifique se requirements.txt está atualizado

4. **Erro de Deploy**
   - Verifique se as APIs estão habilitadas
   - Verifique se o repositório existe

Logs de Debug

```
# Habilitar logs detalhados
export CLOUDSDK_CORE_VERBOSITY=debug
gcloud run deploy ... --verbosity=debug
```

📈 Otimizações de Performance

Configurações Recomendadas

```
gcloud run services update vision-estoque \
    --memory 1Gi \
    --cpu 1 \
    --min-instances 0 \
    --max-instances 10 \
    --concurrency 80 \
    --timeout 300 \
    --region us-central1
```

Monitoramento de Custos

- Configure alertas de billing
- Use `--min-instances 0` para reduzir custos
- Monitore métricas de uso

🔄 Atualizações Futuras

Para atualizar a aplicação:

1. Faça as alterações no código
2. Commit e push para o repositório
3. Execute novamente `./deploy.sh`

📞 Suporte

Para problemas ou dúvidas:
1. Verifique os logs: `gcloud run logs tail vision-estoque --region=us-central1`
2. Consulte a documentação do Cloud Run
3. Verifique as configurações de segurança implementadas

✅ Deploy Seguro Implementado com Sucesso!

Todas as vulnerabilidades foram corrigidas e a aplicação está pronta para produção com as melhores práticas de segurança.