# RENOVAÇÃO DE CERTIFICADO SSL - SALESFORCE COMMERCE CLOUD (SFCC)

## 📋 INFORMAÇÕES GERAIS

**Data de Criação:** $(date)  
**Versão:** 1.0  
**Autor:** Equipe de Desenvolvimento  
**Frequência:** Anual (renovação obrigatória)

## 🎯 OBJETIVO

Este documento fornece instruções detalhadas para renovação de certificados SSL no Salesforce Commerce Cloud (SFCC), utilizando os arquivos .key e .conf existentes do cliente.

## ⚠️ IMPORTANTE - ANTES DE COMEÇAR

* **Renove com antecedência:** Mínimo 2-4 semanas antes da expiração
* **Backup obrigatório:** Sempre faça backup dos certificados atuais
* **Teste primeiro:** Se possível, teste em ambiente de staging
* **Tempo estimado:** 2-4 horas para todo o processo

## 📁 ARQUIVOS NECESSÁRIOS

Você deve ter em mãos: - ✅ certificado.key (chave privada atual) - ✅ certificado.conf (arquivo de configuração) - ✅ Acesso ao Business Manager (BM) do SFCC - ✅ Acesso à CA (Certificate Authority) do cliente

## 🔧 PASSO A PASSO DETALHADO

### **PASSO 1: PREPARAÇÃO DOS ARQUIVOS**

#### 1.1 Verificar arquivos existentes

# Verificar se a chave privada está válida  
openssl rsa -in certificado.key -check -noout  
  
# Verificar data de expiração do certificado atual  
openssl x509 -in certificado.crt -text -noout | grep "Not After"

#### 1.2 Gerar novo CSR (Certificate Signing Request)

# Gerar CSR usando a chave privada existente  
openssl req -new -key certificado.key -out certificado\_renovacao.csr -config certificado.conf  
  
# Verificar o CSR gerado  
openssl req -in certificado\_renovacao.csr -text -noout

**📝 Nota:** O arquivo certificado\_renovacao.csr será enviado para a CA.

### **PASSO 2: SOLICITAÇÃO DO NOVO CERTIFICADO**

#### 2.1 Acessar a CA do cliente

* Entre no portal da CA (DigiCert, Comodo, Let’s Encrypt, etc.)
* Faça login com as credenciais do cliente

#### 2.2 Solicitar renovação

1. **Selecione “Renew Certificate” ou “Renovar Certificado”**
2. **Cole o conteúdo do CSR:**

* cat certificado\_renovacao.csr

1. **Confirme os dados:**
   * Domínio principal
   * Domínios alternativos (SAN)
   * Validação de domínio
   * Período de validade

#### 2.3 Processo de validação

* **Validação de domínio:** Siga as instruções da CA
* **Validação de organização:** Se aplicável
* **Aprovação:** Aguarde a aprovação (geralmente 1-24 horas)

### **PASSO 3: DOWNLOAD DO NOVO CERTIFICADO**

#### 3.1 Baixar o certificado

* Acesse o portal da CA
* Baixe o certificado em formato .crt ou .pem
* **Salve como:** certificado\_novo.crt

#### 3.2 Verificar o certificado

# Verificar data de validade  
openssl x509 -in certificado\_novo.crt -text -noout | grep "Not After"  
  
# Verificar se a chave privada corresponde  
openssl x509 -noout -modulus -in certificado\_novo.crt | openssl md5  
openssl rsa -noout -modulus -in certificado.key | openssl md5

**✅ Os hashes devem ser iguais!**

### **PASSO 4: UPLOAD NO BUSINESS MANAGER (BM)**

#### 4.1 Acessar o BM

1. **URL:** https://[tenant].demandware.net
2. **Login:** Use as credenciais administrativas
3. **Navegue para:** Administration > Organization > Security

#### 4.2 Upload do certificado

1. **Clique em “Certificates” ou “Certificados”**
2. **Selecione “Add Certificate” ou “Adicionar Certificado”**
3. **Preencha os campos:**
   * **Name:** SSL Certificate [Ano] (ex: SSL Certificate 2024)
   * **Certificate:** Faça upload do certificado\_novo.crt
   * **Private Key:** Faça upload do certificado.key (mesmo do ano passado)
   * **Description:** Renovação anual - [Data]

#### 4.3 Configurar o certificado

1. **Associar ao domínio:**
   * Selecione o domínio principal
   * Adicione domínios alternativos se necessário
2. **Configurar datas:**
   * Data de início: Imediata
   * Data de expiração: Conforme o certificado
3. **Ativar:** Marque como “Active” ou “Ativo”

### **PASSO 5: TESTE E VALIDAÇÃO**

#### 5.1 Teste básico

# Testar conectividade HTTPS  
curl -I https://[seu-dominio.com]  
  
# Verificar certificado via navegador  
# Acesse: https://[seu-dominio.com]  
# Verifique se não há avisos de segurança

#### 5.2 Teste completo

1. **Acesse o site via HTTPS**
2. **Verifique em diferentes navegadores:**
   * Chrome
   * Firefox
   * Safari
   * Edge
3. **Teste em dispositivos móveis**
4. **Verifique subdomínios (se aplicável)**

#### 5.3 Verificação de logs

* Acesse os logs do SFCC
* Verifique se não há erros relacionados ao certificado
* Monitore por 24-48 horas

### **PASSO 6: LIMPEZA E FINALIZAÇÃO**

#### 6.1 Remover certificado antigo (após confirmação)

1. **Aguarde 48-72 horas** para confirmar que tudo está funcionando
2. **No BM:** Desative o certificado antigo
3. **Mantenha backup** do certificado antigo por segurança

#### 6.2 Documentação

1. **Atualize este documento** com a data de renovação
2. **Registre no sistema de tickets** do cliente
3. **Notifique a equipe** sobre a renovação

## 🔍 COMANDOS ÚTEIS

### Verificar certificado atual

# Data de expiração  
openssl x509 -in certificado.crt -text -noout | grep "Not After"  
  
# Detalhes completos  
openssl x509 -in certificado.crt -text -noout  
  
# Verificar se a chave privada corresponde  
openssl x509 -noout -modulus -in certificado.crt | openssl md5  
openssl rsa -noout -modulus -in certificado.key | openssl md5

### Gerar CSR

# Gerar CSR  
openssl req -new -key certificado.key -out certificado\_renovacao.csr -config certificado.conf  
  
# Verificar CSR  
openssl req -in certificado\_renovacao.csr -text -noout

### Testar conectividade

# Teste básico  
curl -I https://[dominio.com]  
  
# Teste com verificação de certificado  
curl -I --cacert certificado\_novo.crt https://[dominio.com]

## ⚠️ TROUBLESHOOTING

### Problema: Certificado não funciona

**Solução:** 1. Verifique se a chave privada corresponde ao certificado 2. Confirme se o certificado está ativo no BM 3. Verifique se o domínio está correto 4. Aguarde propagação DNS (até 24 horas)

### Problema: Aviso de segurança no navegador

**Solução:** 1. Verifique se o certificado está ativo 2. Confirme se o domínio está correto 3. Verifique se não há problemas de cadeia de certificados 4. Teste em diferentes navegadores

### Problema: Erro no BM

**Solução:** 1. Verifique se o formato do arquivo está correto (.crt ou .pem) 2. Confirme se a chave privada está no formato correto 3. Verifique se não há caracteres especiais nos nomes dos arquivos 4. Tente fazer upload novamente

## 📞 CONTATOS DE EMERGÊNCIA

* **Suporte SFCC:** [Número do suporte]
* **CA do Cliente:** [Contato da CA]
* **Equipe de Desenvolvimento:** [Contato da equipe]

## 📅 CRONOGRAMA SUGERIDO

| Semana | Atividade |
| --- | --- |
| -4 semanas | Iniciar processo de renovação |
| -3 semanas | Solicitar certificado na CA |
| -2 semanas | Receber e testar certificado |
| -1 semana | Upload no BM e testes finais |
| 0 | Ativação e monitoramento |

## ✅ CHECKLIST FINAL

* Backup do certificado antigo feito
* CSR gerado com sucesso
* Certificado solicitado na CA
* Certificado baixado e verificado
* Upload realizado no BM
* Certificado ativado
* Testes realizados em todos os navegadores
* Logs verificados
* Equipe notificada
* Documentação atualizada

## 📝 NOTAS IMPORTANTES

1. **Sempre use a mesma chave privada** para manter consistência
2. **Renove com antecedência** para evitar interrupções
3. **Teste em ambiente de staging** se possível
4. **Mantenha backups** de todos os certificados
5. **Documente todas as alterações** para futuras renovações

**📄 Este documento deve ser atualizado a cada renovação para manter as informações sempre atuais.**