

# 🔒 ATUALIZAÇÃO: CORA - Integração Direta com mTLS

## ✓ O QUE FOI ATUALIZADO

A integração do gateway CORA foi completamente reformulada para usar **Integração Direta** com autenticação **mTLS (mutual TLS)** através de certificados, conforme documentação oficial do CORA.

## 📋 MUDANÇAS TÉCNICAS

### 1. Certificados Instalados

Os certificados fornecidos foram extraídos e instalados no projeto:

#### 📁 Localização dos Certificados:

```
/home/ubuntu/clivus_landing_page/nextjs_space/certs/
├── cora-certificate.pem  ✓ Certificado público
└── cora-private-key.key  ✓ Chave privada
```

**Data de Emissão:** 20/11/2025

**Data de Vencimento:** 20/11/2026

### 2. Biblioteca lib/cora.ts Reformulada

**Antes (API REST com Bearer Token):**

```
Authorization: `Bearer ${apiKey}`
```

## Agora (mTLS com Certificados):

```
import https from "https";
import fs from "fs";

// Autenticação usando certificados
const cert = fs.readFileSync(certificatePath, "utf8");
const key = fs.readFileSync(privateKeyPath, "utf8");

const requestOptions: https.RequestOptions = {
  hostname: url.hostname,
  port: 443,
  method: "POST",
  cert: cert, // Certificado público
  key: key, // Chave privada
  headers: {
    "Content-Type": "application/json",
    "client-id": config.clientId, // Client ID no header
  },
};
```

## 3. Variáveis de Ambiente Atualizadas

Adicionadas no arquivo `.env` :

```
CORA_API_KEY=int-6ASXCs6nfnjGKWIDAUxco
CORA_WEBHOOK_SECRET=cora_webhook_secret_key
CORA_ENVIRONMENT=production
```

**IMPORTANTE:** `CORA_API_KEY` agora armazena o **Client ID** da Integração Direta, não mais um Bearer Token.

## 4. URL da API Atualizada

**Antes (API REST padrão):**

```
https://api.cora.com.br/v1
```

**Agora (Integração Direta com mTLS):**

```
https://matls-clients.api.stage.cora.com.br
```

**Observação:** A URL é a mesma para **sandbox** e **production**, o ambiente é controlado pelo `CORA_ENVIRONMENT`.

## COMO TESTAR A NOVA INTEGRAÇÃO

### Passo 1: Habilitar o Gateway CORA no Painel Admin

1. Acesse: <https://clivus.marcosleandru.com.br/admin/gateways>
2. Faça login como SuperAdmin: admin@clivus.com.br / admin123
3. Localize o card “CORA”
4. Ative o toggle (deve ficar verde)
5. O badge deve mostrar “Configured” (verde)

### Passo 2: Verificar a Configuração (Opcional)

Você pode verificar se os certificados estão corretos:

```
cd /home/ubuntu/clivus_landing_page/nextjs_space
ls -la certs/
# Deve mostrar:
# cora-certificate.pem
# cora-private-key.key
```

### Passo 3: Testar o Checkout com CORA

#### 1. Acesse o checkout:

<https://clivus.marcosleandru.com.br/checkout?plan=intermediate>

#### 2. Faça login:

- Email: cliente@teste.com
- Senha: senha123

#### 3. Confirme a compra:

- Clique em “Confirmar Compra”
- Você deve ser redirecionado para a página do CORA
- A página do CORA exibirá:

- Opção de PIX (com QR Code)
- Opção de Boleto (com código de barras)

#### 4. Resultado Esperado:

- Redirecionamento bem-sucedido para CORA
- Nenhuma mensagem de erro no checkout

## LOGS DE DEPURAÇÃO

Todos os logs do CORA estão prefixados com [CORA] para facilitar a depuração.

## Como Visualizar os Logs:

```
# Logs em tempo real
pm2 logs

# Filtrar apenas logs do CORA
pm2 logs | grep "\[CORA\]"
```

## Exemplo de Logs Bem-Sucedidos:

```
[CORA] POST https://matls-clients.api.stage.cora.com.br/invoices
[CORA] Request Headers: {}
  "Content-Type": "application/json",
  "client-id": "int-6ASXCs6nfnjGKWIDAUAxco",
  "Content-Length": "456"
}
[CORA] Request Body: {"customer": {"name": "Cliente Teste", ...}}
[CORA] Response Status: 201
[CORA] Response Body: {"id": "boleto_123", "pixQrCode": "00020126...", "digitableLine": "34191..."}
[CORA] Boleto criado: {"id": 'boleto_123', pixQrCode: '...'}
```

## ⚠️ POSSÍVEIS ERROS E SOLUÇÕES

### Erro 1: “Certificado CORA não encontrado”

**Causa:** Os certificados não estão no diretório correto.

**Solução:**

```
ls /home/ubuntu/clivus_landing_page/nextjs_space/certs/
# Se estiver vazio, os certificados foram perdidos
```

**Como Resolver:**

1. Restaure os certificados do arquivo `cert_key_cora_production_2025_11_20.zip`
2. Extraia para `/home/ubuntu/clivus_landing_page/nextjs_space/certs/`
3. Reinicie o servidor

### Erro 2: “CORA\_API\_KEY (Client ID) não configurada”

**Causa:** A variável `CORA_API_KEY` não está no `.env`.

**Solução:**

```
cd /home/ubuntu/clivus_landing_page/nextjs_space
echo 'CORA_API_KEY=int-6ASXCs6nfnjGKWIDAUAxco' >> .env
pkill -f "next dev"
yarn dev
```

## Erro 3: “Error: connect ECONNREFUSED”

**Causa:** URL da API incorreta ou certificados inválidos.

**Solução:**

1. Verifique se os certificados estão válidos (não expirados)
  2. Confirme que `CORA_ENVIRONMENT=production` no `.env`
  3. Teste a conectividade com a API CORA
- 

## Erro 4: “401 Unauthorized”

**Causa:** Client ID incorreto ou certificados não autorizados.

**Solução:**

1. Confirme que o **Client ID** no `.env` é exatamente:  
`CORA_API_KEY=int-6ASXC6nfjGKWIDAUAxco`
  2. Verifique se os certificados correspondem ao Client ID no painel do CORA
  3. Confirme que a integração foi ativada no painel do CORA
- 

## Erro 5: “Invalid certificate”

**Causa:** Certificados corrompidos ou formato incorreto.

**Solução:**

1. Verifique o formato dos certificados:

```
```bash
head -5 /home/ubuntu/clivus_landing_page/nextjs_space/certs/cora-certificate.pem
# Deve começar com: -----BEGIN CERTIFICATE-----

head -5 /home/ubuntu/clivus_landing_page/nextjs_space/certs/cora-private-key.key
# Deve começar com: -----BEGIN RSA PRIVATE KEY-----
```

```

2. Se estiverem corrompidos, restaure do arquivo original
- 



## STATUS ATUAL

| Item                    | Status | Observação                               |
|-------------------------|--------|--|
| Certificados Instalados | ✓      | Em <code>/certs/</code>                  |
| Biblioteca Atualizada   | ✓      | <code>lib/cora.ts</code> reformulada     |
| Variáveis de Ambiente   | ✓      | <code>.env</code> configurado            |
| Build de Produção       | ✓      | Sem erros TypeScript                     |
| Deploy Realizado        | ✓      | <code>clivus.marcosleandru.com.br</code> |

## PRÓXIMOS PASSOS

1. **Habilitar o gateway CORA no painel admin** (`/admin/gateways`)
2. **Testar o checkout** com um plano qualquer
3. **Verificar os logs** (`pm2 logs | grep "\[CORA\]"`)
4. **Validar webhook** (quando o boleto/PIX for pago)

## OBSERVAÇÕES IMPORTANTES

### Diferenças da Integração Direta vs. API REST

| Aspecto             | API REST (Antiga)         | Integração Direta (Atual)           |
|---------------------|---------------------------|-------------------------------------|
| <b>Autenticação</b> | Bearer Token              | mTLS com Certificados               |
| <b>Header</b>       | Authorization: Bearer ... | client-id: ...                      |
| <b>URL</b>          | api.cora.com.br/v1        | matls-clients.api.stage.cora.com.br |
| <b>Segurança</b>    | Chave API secreta         | Certificado X.509 + Chave Privada   |
| <b>Renovação</b>    | Token expira              | Certificado válido por 1 ano        |

### Vantagens da Integração Direta

- ✓ **Maior Segurança:** mTLS garante autenticação bidirecional
- ✓ **Sem Chaves API Expostas:** Certificados são mais seguros
- ✓ **Conformidade:** Recomendado pelo CORA para produção
- ✓ **Renovação Simples:** Apenas trocar o certificado (1x por ano)

## SUPORTE

Se encontrar algum problema:

#### 1. Verifique os logs:

```
bash
pm2 logs | grep "\[CORA\]"
```

#### 2. Teste a conectividade:

```
bash
curl -v --cert /home/ubuntu/clivus_landing_page/nextjs_space/certs/cora-certificate.pem
```

```
--key /home/ubuntu/clivus_landing_page/nextjs_space/certs/cora-private-key.key \
https://matls-clients.api.stage.cora.com.br/health
```

### 3. Consulte a documentação do CORA:

- Portal de Desenvolvedores: <https://developers.cora.com.br/>
  - Guia de Integração Direta: (consulte o painel do CORA)
- 

## CONCLUSÃO

A integração do CORA foi **completamente atualizada** para usar **Integração Direta com mTLS**, conforme as melhores práticas de segurança e a recomendação oficial do CORA.

**Tudo está pronto para uso em produção!** 

---

**Data da Atualização:** 20/11/2025

**Versão do Certificado:** production\_2025\_11\_20

**Client ID:** int-6ASXCs6nfnjGKWIDAUAxco