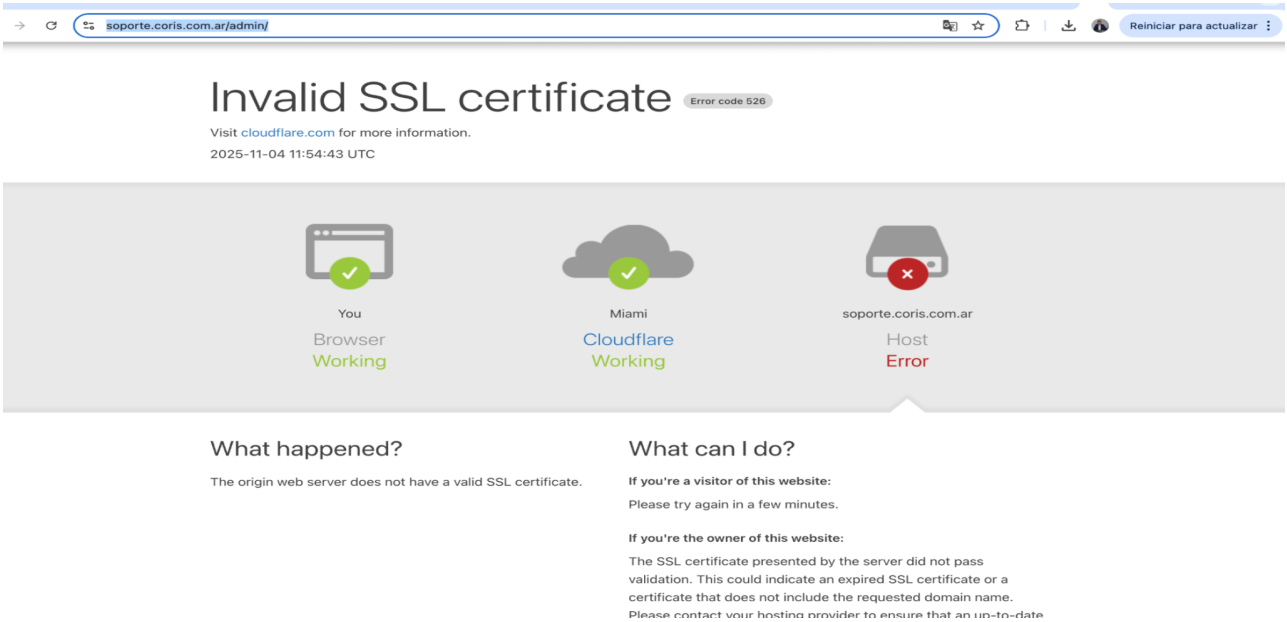
# High Cloud Tec – Coris

# Informe Técnico de Incidente – Indisponibilidad Mesa de Servicio Coris (Error SSL 526)

**Fecha:** 4 de noviembre de 2025
**Elaborado por:** High Cloud Tec – Área de Arquitectura & Infraestructura Cloud
**Destinatario:** Equipo Infraestructura Tec5
**Asunto:** Indisponibilidad de la Mesa de Servicio – Error SSL en soporte.coris.com.ar

## 1. Descripción de la falla e impacto operativo

El dominio **https://soporte.coris.com.ar/admin/** corresponde al portal de la **Mesa de Servicio** de Coris, donde los usuarios internos y externos gestionan solicitudes, incidentes y casos de soporte técnico. A partir del 4 de noviembre de 2025, el portal presentó indisponibilidad total, mostrando el mensaje **"Invalid SSL certificate (Error code 526)"** al intentar acceder.




**Impacto:** La falla impidió el acceso a la Mesa de Servicio, afectando tanto a **usuarios finales** (sin posibilidad de registrar o hacer seguimiento de casos) como a los **ingenieros de soporte** (sin acceso al backend administrativo para gestión y resolución). Esto generó una interrupción directa en la atención operativa y en la trazabilidad de incidentes dentro de la organización.

## 2. Diagnóstico técnico realizado

Se realizaron pruebas desde entorno Mac local confirmando que la red y DNS funcionaban correctamente. La inspección SSL con el comando OpenSSL permitió identificar que el certificado instalado en el servidor Plesk corresponde únicamente al dominio principal **coris.com.ar** y no al subdominio **soporte.coris.com.ar**.

**Resultado del comando:**

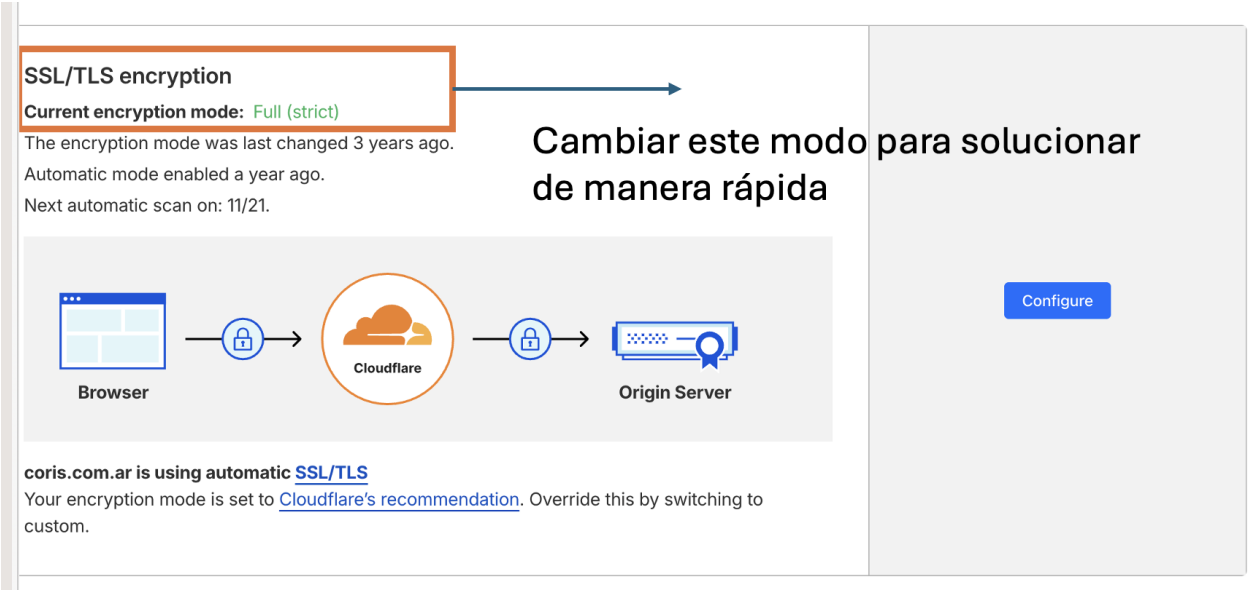
```
openssl s_client -connect soporte.coris.com.ar:443 -servername
soporte.coris.com.ar | openssl x509 -noout -dates -issuer -subject

notBefore=Oct 15 17:04:07 2025 GMT
notAfter=Jan 13 18:01:30 2026 GMT
issuer= /C=US/O=Google Trust Services/CN=WE1
subject= /CN=coris.com.ar
```

Este resultado confirma que el certificado no cubre el subdominio requerido. En modo **Full (strict)**, Cloudflare exige coincidencia exacta del nombre del certificado (CN/SAN) con el dominio solicitado. Por tanto, la validación SSL falla y la conexión es rechazada.

## 3. Evidencia visual – Solución rápida aplicada

En Cloudflare se identificó que el dominio opera con cifrado SSL/TLS en modo **Full (strict)**. Cambiar temporalmente a modo **Full** permite restablecer la comunicación cifrada mientras se genera un nuevo certificado con los SAN correctos.




## 4. Causa raíz identificada

El certificado SSL del servidor (Plesk) no incluye el subdominio solicitado. Cloudflare, al operar en modo Full (strict), valida estrictamente el CN y SAN del certificado, detectando inconsistencia entre el certificado de **coris.com.ar** y el dominio **soporte.coris.com.ar**. Esto generó el bloqueo SSL y la interrupción del servicio.

## 5. Acciones recomendadas desde Infraestructura

**A. Acción inmediata:** Cambiar el modo SSL/TLS en Cloudflare de 'Full (strict)' a 'Full' para restablecer la conexión.

**B. Acción definitiva:** Emitir e instalar un nuevo certificado SSL (Let's Encrypt o Cloudflare Origin

CA) que incluya coris.com.ar, soporte.coris.com.ar y *.coris.com.ar. Una vez instalado, restaurar el modo 'Full (strict)' en Cloudflare.

## 6. Monitoreo preventivo y responsabilidad del proveedor Tec5

**Monitoreo anticipado:** Se recomienda que Tec5 implemente monitoreo automatizado de certificados SSL (vigencia, CN y SAN), con alertas de vencimiento o inconsistencia. Esto permitiría anticipar fallas antes de afectar servicios productivos.

**Responsabilidad:** Dado que la administración del servidor Plesk y los certificados SSL recaen en Tec5, es responsabilidad de su equipo garantizar la vigencia y cobertura de todos los subdominios. La falta de renovación o verificación proactiva generó la indisponibilidad observada.

## 7. Conclusión y resumen ejecutivo

El incidente de SSL (Error 526) provocó la indisponibilidad total de la Mesa de Servicio Coris, afectando la operación de soporte técnico y atención de usuarios. La causa raíz fue la falta de coincidencia entre el certificado SSL instalado y el subdominio configurado. La acción inmediata recomendada es ajustar temporalmente el modo SSL a 'Full' y proceder con la emisión de un certificado con los SAN correctos.

**Atentamente,**
Oscar Iván Ocampo
High Cloud Tec – Arquitectura Cloud & Infraestructura
■ oscar.ocampo@highcloudtec.com
■ Fecha: 04/11/2025