Guía paso a paso para resolver el error ERR_SSL_FALLBACK_BEYOND_MINIMUM_VERSION

El error **ERR_SSL_FALLBACK_BEYOND_MINIMUM_VERSION** indica que tu navegador no puede establecer una conexión segura con un servidor porque este último utiliza versiones antiguas y desactualizadas del protocolo SSL/TLS. Este problema puede deberse a configuraciones desactualizadas del servidor, sistemas operativos obsoletos o problemas con certificados SSL. Sigue esta guía para solucionar el problema.

🔍 Puntos clave de esta guía

1. Verificar el soporte de protocolos SSL/TLS en el servidor.
2. Ajustar configuraciones de seguridad en navegadores y servidores.
3. Actualizar el sistema operativo y software relacionado.
4. Identificar y eliminar software o configuraciones problemáticas.
5. Contactar al propietario del sitio web en situaciones específicas.

🛠️ Guía detallada: Cómo solucionar el error

1. Comprender el origen del problema

El error se produce cuando el cliente (tu navegador) detecta que el servidor usa un protocolo de cifrado no compatible, como versiones antiguas de SSL (ej., SSL 2.0, SSL 3.0) o versiones de TLS que están deshabilitadas en navegadores modernos.

---

2. Actualizar el servidor para admitir TLS 1.2 o TLS 1.3

El protocolo SSL está obsoleto y ha sido reemplazado por TLS (Transport Layer Security). Asegúrate de que el servidor web que estás intentando acceder tenga soporte para TLS 1.2 o TLS 1.3.

Pasos recomendados:

1. Si tienes control del servidor web:
    - Edita los archivos de configuración como `nginx.conf` o `apache.conf`.
    - Habilita solamente protocolos TLS 1.2 o TLS 1.3 en los ajustes.
    - Desactiva SSL 2.0, SSL 3.0 y TLS 1.0/1.1.
2. Herramientas útiles para verificar la configuración del servidor:
    - SSL Labs: Permite realizar pruebas completas para identificar configuraciones deficientes en SSL/TLS.
    - Test your server: Herramienta gratuita para analizar la configuración de tu servidor.

---

3. Configurar el navegador para protocolos más modernos

Los navegadores modernos como Chrome, Firefox y Edge no admiten protocolos antiguos por defecto. Si estás utilizando navegadores antiguos, **actualízalos inmediatamente**.

Extensiones útiles recomendadas:

- Instala NordVPN para mantener conexiones cifradas con protocolos compatibles.
- Usa un gestor de contraseñas como NordPass Secure para administrar sitios seguros.

---

4. Actualizar el sistema operativo

El error puede surgir cuando el dispositivo o sistema operativo no admite protocolos más modernos. Para garantizar compatibilidad:

1. **Windows**:
    - Actualiza a la versión más reciente de Windows 10/11.
    - Importante: TLS 1.2 está habilitado por defecto solo en versiones recientes.
    - Si es necesario, puedes habilitarlo manualmente vía el Editor de Registro.

      ```
      [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp]
      "DefaultSecureProtocols"=dword:00000A00
      ```

2. **MacOS**:
    - Asegúrate de estar en **MacOS Catalina** o versiones posteriores.
    - Verifica certificados actuales utilizando **Keychain Access**.

3. **Linux**:

- Actualiza OpenSSL a su última versión:

  ```
  sudo apt-get update
  sudo apt-get install openssl
  ```

---

5. Eliminar certificados problemáticos o corruptos

1. Accede a las configuraciones de certificados de tu navegador o sistema operativo.
2. Verifica y elimina certificados expirados o no confiables.
3. Utiliza herramientas como MiniTool ShadowMaker para realizar backups antes de realizar cambios.

---

6. Verifica el balanceador de carga y el firewall

Los balanceadores de carga o firewalls que no admiten protocolos modernos también pueden causar el error. Actualiza estos sistemas y verifica su compatibilidad con TLS 1.2 o TLS 1.3.

---

7. Desactiva software antivirus que interfiere

Algunos antivirus se exceden al intentar escanear sitios HTTPS, interrumpiendo la conexión. Si sospechas que tu antivirus está causando el problema:

- Desactiva temporalmente la función de "protección HTTPS".
- Si usas herramientas avanzadas, prueba alternativas como **Malwarebytes** (consigue un descuento aquí: Malwarebytes 25% Off).

---

8. Eliminar software innecesario (como Superfish)

Si utilizas dispositivos antiguos como Lenovo, es posible que existan configuraciones redundantes o software como **Superfish** que causan problemas de certificados.

Solución oficial:

- Descarga la herramienta de eliminación desde Lenovo Support.

---

9. Probar en modo incógnito

Abre la página en modo incógnito o desactiva extensiones del navegador (como bloqueadores de anuncios). Es posible que una extensión mal configurada esté bloqueando el acceso.

---

10. Contactar al soporte del sitio web

Si todo falla, contacta con el propietario del sitio web. Solicita que actualicen su configuración o proporcionen instrucciones sobre compatibilidad con sistemas obsoletos.

Preguntas frecuentes (FAQ)

❓ ¿Por qué ocurre el error ERR_SSL_FALLBACK_BEYOND_MINIMUM_VERSION?

Esto ocurre porque el navegador detecta que el servidor utiliza una versión obsoleta del protocolo SSL/TLS.

❓ ¿Puedo deshabilitar el error desde el navegador?

No. La solución requiere corregir el protocolo del servidor o actualizar sistemas y navegadores en el cliente.

❓ ¿Qué herramientas recomendadas puedo usar para solucionar este problema?

1. SSL Labs para analizar servidores.
2. Malwarebytes 25% OFF para problemas de software.
3. EaseUS Backup Center para respaldar configuraciones.

❓ ¿Es seguro desactivar antivirus que interfiere con HTTPS?

Desactívalo temporalmente solo para probar la conexión. Nunca lo dejes deshabilitado permanentemente.

Siguiendo esta guía paso a paso, deberías poder resolver el error **ERR_SSL_FALLBACK_BEYOND_MINIMUM_VERSION** en la mayoría de los casos. Recuerda verificar tus configuraciones y mantener tu sistema actualizado para prevenir futuros problemas relacionados con cifrado y seguridad.