

Manejo de Errores

Aprende a identificar y resolver errores al usar API Gateway

Anonymous · 27/08/2026

Manejo de Errores

Los errores son **normales** al integrar; lo clave es saber **dónde mirar: código HTTP** (ej. 200, 401, 429), **cuerpo** de la respuesta (mensaje) y **cabeceras** (límites, tiempos, señales de sesión). En la [documentación interactiva](#), con **Try it out**, sueles ver **todo junto**.

Códigos de error principales

Tabla de referencia rápida

Código	Nombre	Significado	Acción habitual
400	Bad Request	Petición inválida o no procesada	Revisar JSON, parámetros y formato
401	Unauthorized	Token de conexión inválido, credenciales SII incorrectas o sesión SII	Token, RUT/clave, certificado o sesión
402	Payment Required	Créditos insuficientes o IP compartida con otra conexión	Cargar créditos o revisar la IP de origen
403	Forbidden	Sin permiso al recurso u operación	Productos de la conexión o estado de cuenta
404	Not Found	Ruta o recurso no encontrado	URL y parámetros
405	Method Not Allowed	Método HTTP incorrecto	GET vs POST, etc.
406	Not Acceptable	Formato de respuesta no aceptado	Parámetro <code>formato</code> o cabeceras
409	Conflict	Conflicto con datos en el SII	Revisar datos enviados
410	Gone	Recurso ya no disponible en la API	Actualizar según documentación vigente
423	Locked	Cuenta bloqueada por términos	Revisar términos y soporte
429	Too Many Requests	Límite de uso alcanzado	Esperar, revisar cabeceras y plan

Nota

Con el tiempo pueden añadirse o ajustarse códigos. Diseña tu software para tratar también un **caso por defecto** cuando llegue un código que no esperabas.

Bloqueo de la cuenta

Rige el uso de la plataforma según los [términos y condiciones](#). Entre los factores que pueden afectar están **muchas respuestas 429** por un patrón de uso.

Identificando errores

Dónde está la información

1. **Status code** (arriba en la respuesta de la herramienta o en la primera línea de `curl -i`).
2. **Response body** — mensaje en JSON u otro formato.
3. **Response headers** — límites, `Retry-After`, créditos, señales de sesión (ver [Tu primera petición](#)).

Ejemplo visual de error 401 (ilustrativo)

Code: 401 Unauthorized

Response body:

```
{
  "detail": "Token de conexión inválido."
}
```

Response headers:

```
content-type: application/json
X-RateLimit-Limit: 1000
X-RateLimit-Remaining: 999
```

El texto de `detail` puede variar según idioma y caso.

Interpretando cabeceras de respuesta

Rate limiting (muy frecuente)

Cabecera	Significado	Ejemplo
X-RateLimit-Limit	Tope de la ventana que aplica	1000
X-RateLimit-Remaining	Peticiones que aún puedes hacer	847
X-RateLimit-Reset	Momento (Unix) en que se renueva la ventana	1735689600

En respuestas **exitosas**, mira **X-RateLimit-Remaining** para reducir sorpresas antes de llegar al **429**.

Cuando llegas al límite (429)

Cabecera	Significado	Ejemplo
Retry-After	Segundos sugeridos antes de reintentar	3600

Errores comunes y soluciones

Error 401: token de conexión

```
{
  "detail": "Token de conexión inválido."
}
```

O mensajes genéricos de no autenticado.

Solución: usa la cabecera exacta **Authorization: Token <tu_token>** (palabra Token, espacio, clave). El token se genera en [Gestionar conexión](#); si **regeneraste** el token, actualiza tu integración.

Error 401: credenciales SII (RUT/clave)

Solución: verificar en www.sii.cl; formato de RUT con guión y sin puntos; JSON `auth.pass` completo.

Error 401: sesión SII / reautenticación

```
{
  "code": 401,
  "detail": "Se debe volver a autenticar al usuario en la sesión del SII."
}
```

Cabecera útil: X-Auth-Session-Problem: 1.

Solución inmediata: revisa la sección **Control de caché de sesión** más abajo (parámetro `auth_cache` **solo** cuando corresponda).

Error 429: demasiadas peticiones

```
{
  "detail": "Too Many Attempts."
}
```

Solución:

1. Lee **Retry-After** si viene en cabeceras.
2. Espera esos segundos antes de reintentar en masa.
3. Revisa plan y optimiza frecuencia de llamadas.

Error 402: créditos insuficientes

```
{
  "status": 402,
  "code": "error",
  "detail": "Créditos insuficientes para realizar la consulta. Créditos disponibles:
0.500, costo de esta operación: 1.000"
}
```

Causa: el saldo de la conexión no alcanza para cubrir el costo de la operación solicitada. El mensaje incluye ambos valores, así que sabes exactamente cuánto falta.

Solución: compra créditos en [Gestionar conexión](#). El costo en créditos de cada recurso está en [Precios](#) y en la [documentación de la API](#).

Anticípate

La cabecera **X-Stats-Credits-Remaining** viene en las respuestas exitosas con el saldo que te queda. Monitoréala para recargar antes de quedarte sin créditos a mitad de un proceso.

Error 402: IP en uso por otra conexión

```
{
  "status": 402,
  "code": "error",
  "detail": "No está permitido realizar consultas desde la IP 203.0.113.99, ya que se
encuentra en uso por otra conexión. Para consultar desde esta IP debe realizar la
compra de créditos."
}
```

Causa: las conexiones que aún **no han pagado ningún cobro** solo pueden consultar desde una IP que ninguna otra conexión haya utilizado. Si consultas desde una IP que ya está en uso, la petición se rechaza.

Solución: realiza la **compra de créditos**. Una vez registrado el pago, la conexión queda habilitada para consultar desde cualquier IP, incluidas las compartidas.

Alternativa mientras tanto: consultar desde una IP que no esté siendo usada por otra conexión.

Error 400: petición mal formada

Causas: JSON inválido, campos obligatorios faltantes, tipos incorrectos.

En la documentación interactiva: revisa el esquema del body; los editores suelen marcar errores.

Control de caché de sesión (SII)

Si envías **RUT/clave** o **certificado** en el cuerpo, API Gateway puede **reutilizar la sesión del SII** un tiempo (del orden de **2 horas**): es **normal**, ayuda al **rendimiento** y evita **demasiados logins** seguidos al SII.

Comportamiento por defecto

Tras un login exitoso, las siguientes consultas pueden **reaprovechar** la sesión; **no** debes forzar un login nuevo en cada llamada si todo funciona.

Forzar nueva sesión (auth_cache)

Ante errores de **reautenticación** o cabecera **X-Auth-Session-Problem: 1**, revisa la **documentación del endpoint**; a veces indican añadir a la URL algo como:

```
?auth_cache=0
```

Ejemplo de idea (la ruta real es la de tu operación):

```
POST
https://app.apigateway.cl/api/v2/sii/bhe/emitidas/documentos/11111111-1/202401?auth_cache=0
```

Cuándo usarlo: tras **cambiar la clave** del SII; cuando el error indica claramente problema de sesión y los reintentos normales fallan; o en **depuración puntual**.

Advertencia

No uses `auth_cache=0` en **todas** las peticiones de producción. Cada forzado puede equivaler a un nuevo inicio de sesión en el SII y aumentar riesgo de bloqueos o lentitud.

Los valores permitidos de `auth_cache` y su significado están en la **documentación interactiva** de cada operación.

Estrategias de prevención

1. Monitoreo de límites

Si **X-RateLimit-Remaining** baja mucho, **espacia** las llamadas y valora **caché** en tu sistema para no

repetir la misma consulta.

2. Sesiones SII

No abuses de `auth_cache=0`. Si aparece `X-Auth-Session-Problem`, trata la sesión antes de insistir a ciegas.

3. Validación previa

Antes de enviar, comprueba **JSON** bien formado, **campos obligatorios** presentes, **tipos** correctos y **token** vigente.

Last updated on 21/08/2026