Focaltec

GUÍA DE USO

DEL API Y POLÍTICA DE USO JUSTO

Código: FOC-DI-POL-13

Revisión: 01

Elaborado por:	Revisado y aprobado por:
Director de Infraestructura y Seguridad y Responsable del SGSI	Director General

Objetivo

Que el cliente conozca y aplique las buenas prácticas en el uso del API del Portal de Proveedores, garantizando un manejo seguro, eficiente y alineado con los lineamientos establecidos para optimizar la integración de sus procesos.

Alcance

Área de proyectos, desarrollo, infraestructura, soporte y clientes, que usan el API de Portal de Proveedores.

Introducción

Este documento describe las recomendaciones, lineamientos y mejores prácticas para el consumo del **API de Focaltec Portal De Proveedores**.

En este documento se entiende por **uso eficiente y responsable del API** aquel que permite integrar procesos de forma segura, controlada y alineada con las capacidades técnicas del servicio. Esto implica consumir únicamente los datos necesarios, evitar llamadas excesivas o repetitivas, implementar estrategias de reintento adecuadas y respetar los tiempos de respuesta del sistema.

Para reforzar estos principios, se aplicarán **restricciones técnicas de frecuencia** que regulan la cantidad de solicitudes permitidas por unidad de tiempo. Esta medida busca proteger la disponibilidad del servicio, prevenir sobrecargas involuntarias y asegurar una experiencia equitativa para todos los consumidores del API.

Uno de los pilares principales de la seguridad de la información es la disponibilidad de la información de nuestros clientes en todo momento. El uso inadecuado de las APIs que Focaltec pone a la disposición de sus clientes pueden afectar el desempeño y disponibilidad de la información. Es por ello que Focaltec en todo momento se reserva el derecho de bloquear el acceso a sistemas que, por su mal diseño o implementación, pongan en riesgo la disponibilidad de la plataforma.

Consideraciones Generales

Nuestro API ha sido diseñado para ofrecer flexibilidad y alto rendimiento, para garantizar la estabilidad y la calidad del servicio hay que considerar lo siguiente:

Rate Limit

- Tiene un rate limit de 500 peticiones por minuto por dirección IP.

Paginación

- El tamaño máximo permitido por página es de **200 elementos por solicitud.**
- Utilizar paginación en todas las consultas que involucren grandes volúmenes de datos.

Rango de Fechas

- El rango máximo permitido por consulta es de **30 días naturales.**
- Para consultas históricas más amplias, se deberán realizar múltiples solicitudes segmentadas.

Frecuencia de las solicitudes

- Consultas para una entidad (OC, Entradas, CFDIs, Reportes) no deben repetirse en intervalos de tiempo. Se debe implementar webhooks para que se hagan las consultas cuando cambien a un estatus que genere una consulta.

Porcentaje de errores 4xx

- No más del 20% de las peticiones realizadas por el Cliente o Integrador podrán resultar en respuestas HTTP 4xx dentro del periodo de medición aplicable.

Política de Uso Justo

Tomando en cuenta las consideraciones generales, todos los clientes deben adherirse a una política de uso. Esto implica:

- Evitar realizar solicitudes excesivas o innecesarias en alta frecuencia.
    - Por ejemplo, pedir la consulta del estatus de las Órdenes de Compra cada 5 minutos durante todo el día.
- No ejecutar consultas masivas que puedan impactar el desempeño del sistema.
    - Ejemplo, consultar los CFDIs del último mes durante 3 veces al día.
- Evitar patrones de extracción completa de datos. Diseñar integraciones que no dependan de servicios configurados por plazos de tiempo sino que se implementen webhooks que disparen consultas cuando hace sentido hacerlas.

Mejores Prácticas

Paginación

- Utilizar tamaños de página adecuados (hasta el máximo permitido)
- Evitar solicitudes que intenten recuperar grandes volúmenes en una sola llamada.

Estrategias de Reintento

- Implementar reintentos con *exponential backoff* (esperar cada vez más tiempo entre intentos).
- Evitar ciclos agresivos de reintentos, entendidos como múltiples solicitudes consecutivas ante errores sin aplicar lógica de espera, validación del tipo de error o límite de intentos.

Sincronización de Datos

- Priorizar sincronizaciones incrementales en lugar de cargas completas.
- Consultar únicamente datos nuevos o modificados.

Adecuado manejo de errores

- Se debe hacer un manejo adecuado de errores y cuando la plataforma regrese un error del tipo "Elemento duplicado", los cuales, no deben de seguir intentando estas llamadas.

Monitoreo y Prevención de Abuso

Monitoreamos continuamente los patrones de uso del API para asegurar la estabilidad del servicio.

Nos reservamos el derecho de:

- Analizar patrones de uso inusuales o potencialmente abusivos.
- Contactar a clientes cuyo consumo impacte negativamente en la plataforma.
- Aplicar restricciones temporales o permanentes en caso necesario.

Cambios futuros

Como parte de la política de uso justo, el servicio podrá aplicar restricciones técnicas adicionales que regulen el volumen, frecuencia y tipo de operaciones permitidas. Estas medidas buscan proteger la estabilidad del API, prevenir abusos involuntarios y asegurar una experiencia equitativa para todos los consumidores. Las restricciones podrán ajustarse conforme evolucionen los patrones de uso y las capacidades técnicas del servicio. Cualquier cambio será comunicado con anticipación.

Soporte

Si tu caso de uso requiere un alto volumen de consumo o tienes necesidades específicas de integración, te invitamos a contactarnos:

📧 **soporte@focaltec.com**

Nuestro equipo estará disponible para ayudarte a diseñar una integración óptima.

Notificación y Restricciones

En caso de detectar un uso inadecuado del API que afecte la estabilidad, disponibilidad o desempeño del servicio, se seguirá el siguiente procedimiento:

1. Detección y análisis

- Se identifican patrones de uso inusuales, excesivos o que incumplan las buenas prácticas definidas.
- Se realiza un análisis técnico para confirmar el impacto y la causa del comportamiento.

2. Notificación preventiva (Primer aviso)

Se notificará al cliente vía correo electrónico describiendo:

- El comportamiento detectado.
- El impacto generado.
- Las recomendaciones para corregirlo.
- Se indicará en el correo el plazo de corrección según sea el caso.

3. Seguimiento

- Se monitorea el comportamiento del cliente durante el periodo de corrección.
- En caso de mejora, no se aplican medidas adicionales.

4. Advertencia formal (Segundo aviso)

Si el comportamiento persiste, se emite una advertencia formal indicando:

- Incumplimiento de la política de uso justo.
- Posibles medidas correctivas.
- Se establece un nuevo plazo de corrección más corto.

5. Aplicación de medidas

Si el uso indebido continúa, se podrán aplicar las siguientes acciones:

- Limitación temporal de consumo (rate limiting).
- Throttling de solicitudes.
- Bloqueo parcial de endpoints específicos.
- Suspensión temporal del acceso al API.

6. Suspensión o bloqueo definitivo

- En casos críticos o reincidentes, se podrá suspender de manera indefinida el acceso al API.

7. Restablecimiento del servicio

El acceso podrá restablecerse una vez que el cliente:

- Demuestre haber corregido su integración.
- Se comprometa a cumplir con las políticas establecidas.

HISTÓRICO DE LAS MODIFICACIONES		
No. de Revisión	**Fecha**	**Modificación**
00	27/03/2026	Edición inicial
01	02/06/2026	Se agrega en Consideraciones Generales el porcentaje de errores 4xx