Facturación Electrónica

Estándares de Comportamiento Esperado en la Integración con el Sistema

Ventanas de Mantenimiento y Procesos de Contingencia



Guía de Referencia para Contribuyentes Emisores Electrónicos y Proveedores Tecnológicos

Gerencia de Facturación

IMPUESTOS INTERNOS

Tabla de Contenido

1. PROPÓSITO 3
2. ALCANCE 3
3. MARCO LEGAL 3
4. DIRETRICES OPERATIVAS POR ÁREA DE INTEGRACIÓN 4
5. VENTANAS DE MANTENIMIENTO 10
   - 5.1 CANAL OFICIAL DE MONITOREO DE DISPONIBILIDAD 10
   - 5.2 COMPORTAMIENTO ANTE INDISPONIBILIDAD 10
   - 5.3 REANUDACIÓN CONTROLADA TRAS LA RESTAURACIÓN 11
6. PROCESOS DE CONTINGENCIA DEL CONTRIBUYENTE 11
   - 6.1 TIPOS DE CONTINGENCIA RECONOCIDOS POR LA DGII 11
   - 6.2 CONSIDERACIONES NORMATIVAS CLAVE 12
7. CANALES DE VERIFICACIÓN Y REFERENCIAS 12

1. Propósito

Esta guía establece los patrones de comportamiento, principios operativos y lineamientos técnicos que deben observar los contribuyentes, proveedores de servicios, desarrolladores e integradores en el uso de la solución tributaria de Facturación Electrónica de la Dirección General de Impuestos Internos (DGII) de la República Dominicana. Su propósito es promover una interacción consistente, segura, eficiente y alineada con los objetivos de la administración tributaria, garantizando la correcta emisión, recepción, validación, consulta e intercambio de documentos fiscales electrónicos. Para ello, organiza sus recomendaciones en cinco dimensiones fundamentales para una integración correcta, segura y sostenible:

- Cumplimiento y autorización
- Seguridad e identidad técnica
- Uso correcto de los servicios
- Manejo de errores y continuidad
- Mantenimiento y contingencia

Asimismo, esta guía busca orientar a los equipos técnicos de los contribuyentes emisores electrónicos y proveedores tecnológicos en la implementación de integraciones alineadas con las mejores prácticas de consumo de servicios, fomentando un uso responsable de los recursos compartidos y contribuyendo a mantener la disponibilidad, estabilidad y calidad del servicio para todo el ecosistema de Facturación Electrónica.

2. Alcance

- **Contribuyentes Electrónicos** que integran directamente sus sistemas de facturación con los servicios de Factura Electrónica de la DGII.

- **Proveedores Tecnológicos** que desarrollan, mantienen o distribuyen software de Facturación Electrónica utilizado por contribuyentes en la República Dominicana.

- **Equipos Técnicos** responsables del diseño, implementación y mantenimiento de integraciones con los diferentes servicios de Facturación Electrónica.

3. Marco Legal

Las buenas prácticas descritas en esta guía no son sugerencias opcionales - son directrices de comportamiento que la Dirección General de Impuestos Internos emite en ejercicio de sus facultades normativas y de administración tributaria, con fundamento en el ordenamiento jurídico vigente.

> **Base normativa:**
>
> **Ley 11-92** - Código Tributario de la República Dominicana. Faculta a la DGII para establecer obligaciones, procedimientos y medidas correctivas en el ejercicio de sus funciones de administración y fiscalización tributaria.

Ley 32-23 - Ley de Facturación Electrónica. Establece el marco legal del sistema eCF, las obligaciones de los contribuyentes emisores y los proveedores tecnológicos certificados, y habilita a la DGII para dictar las normas técnicas y operativas necesarias para el funcionamiento del sistema.

Decreto 587-24 - Reglamento de aplicación de la Ley 32-23. Define los procedimientos, requisitos técnicos y condiciones operativas bajo las cuales deben integrarse y operar los contribuyentes y proveedores en el sistema de facturación electrónica.

Norma General 01-2020 - Norma técnica de comprobantes fiscales electrónicos emitida por la DGII. Establece las especificaciones de integración, los esquemas de validación y los estándares que deben cumplir los sistemas de los contribuyentes y sus proveedores tecnológicos.

Ley 53-07 - Ley sobre Crímenes y Delitos de Alta Tecnología. Tipifica las conductas que afectan la integridad y disponibilidad de los sistemas de información, y fundamenta las responsabilidades que pueden derivarse del comportamiento anómalo sobre plataformas tecnológicas del Estado.

Principio de responsabilidad compartida

El sistema atiende de forma simultánea a miles de contribuyentes electrónicos, por lo que los recursos de la plataforma deben considerarse compartidos. En consecuencia, el tráfico generado por una integración, las conexiones abiertas, los envíos concentrados o las consultas frecuentes pueden afectar o reducir la capacidad disponible para los demás contribuyentes. Por ello, la DGII se reserva el derecho de aplicar las medidas de seguridad preventivas o de limitación que resulten necesarias según el escenario.

Nota de aplicación

Las directrices de esta guía aplican a ambos modelos de operación tributaria: el modelo B2B (emisor a receptor electrónico, asíncrono) y el modelo B2C (emisor a consumidor final, en línea). Donde aplique exclusivamente a uno de los modelos, se indicará expresamente.

4. Directrices Operativas por Área de Integración

La siguiente sección consolida las directrices de comportamiento aplicables a los contribuyentes electrónicos que interactúan con los servicios de Facturación Electrónica en el entorno de producción. Estructurada por áreas funcionales y conforme al flujo operativo de los procesos, establece los comportamientos esperados para un consumo adecuado de los servicios, así como las prácticas no autorizadas que constituyen un uso indebido o exceden los límites de la autorización concedida por la DGII.

Área	Requerido	Prohibido
	• Reconocer que Facturación Electrónica constituye una **plataforma compartida** y que toda integración tiene	• Asumir que el servicio puede utilizarse sin límites ni

Plataforma compartida	responsabilidad sobre el uso adecuado de los servicios y la preservación de su estabilidad y disponibilidad para los demás contribuyentes. • Mantener patrones de consumo controlados. Los comportamientos de alto impacto, tales como ráfagas de conexiones, envíos masivos concentrados en períodos reducidos y consultas de estado de alta frecuencia (polling agresivo), son monitoreados por la DGII y cuando estos patrones puedan comprometer la estabilidad o disponibilidad de los servicios, podrán derivar en medidas de control, incluyendo limitaciones de acceso, con el objetivo de preservar la continuidad del ecosistema. • Asegurar que toda automatización, robot o proceso asistido por inteligencia artificial opere con límites de consumo proporcionales al volumen real de operaciones del contribuyente, incorporando los controles necesarios de concurrencia, frecuencia y reintentos.	considerar su naturaleza compartida. • Generar tráfico desproporcionado que afecte la disponibilidad del servicio para otros contribuyentes. • Ignorar las medidas de control o limitación aplicadas por la DGII ante comportamientos anómalos o de alto impacto. • Generar tráfico automatizado que no pueda atribuirse a un proceso legítimo, autorizado y trazable.
Marco normativo	• Conocer y cumplir: Ley 32-23, Decreto 587-24 (Arts. 40-43), Norma General 01-2020. • Consultar la documentación técnica oficial publicada en el portal dgii.gov.do antes de implementar cualquier integración.	• Implementar o modificar integraciones sin revisar previamente la normativa y documentación técnica oficial vigente. • Basar la integración en interpretaciones informales, documentación desactualizada o fuentes no oficiales. • Alegar desconocimiento normativo como justificación de incumplimientos operativos o técnicos.
Ambientes FE	• **Pre-certificación:** pruebas de adecuación, integración de desarrollos, carga y estrés. • **Certificación:** proceso formal de habilitación como emisor electrónico ante la DGII. • **Producción:** envíos con validez fiscal. Solo para integraciones certificadas. • Validar el comportamiento de automatizaciones, robots o agentes inteligentes en el ambiente correspondiente antes de su uso en producción.	• Cruzar propósitos entre ambientes. • Ejecutar pruebas en producción. • Cruzar credenciales entre ambientes. • Desplegar automatizaciones de emisión, consulta o reintento en producción sin validación previa en el ambiente correspondiente. • Permitir que un mismo agente o automatización reutilice

	• Mantener separadas las configuraciones, credenciales y reglas de decisión por ambiente, también para procesos automáticos.	credenciales, configuraciones o lógicas entre ambientes sin control explícito.
Modelo B2B vs B2C	• Distinguir explícitamente ambos modelos en la integración: B2B asíncrono (requiere consulta posterior), B2C síncrono (respuesta en el mismo envío). • Parametrizar las automatizaciones para que distingan correctamente entre flujos B2B y B2C. • Asegurar que cualquier proceso automático respete la naturaleza asíncrona de B2B y la respuesta en línea de B2C.	• Aplicar patrones B2B al modelo B2C ni viceversa. • Permitir que una automatización aplique la misma lógica de envío, validación, consulta o reintento a modelos B2B y B2C sin diferenciación. • Diseñar agentes automáticos que asuman respuesta definitiva en operaciones B2B o que introduzcan consultas innecesarias en B2C.
Transporte seguro	• Usar exclusivamente HTTPS (TLS) para todas las comunicaciones con los servicios de Facturación Electrónica. • Debe protegerse la transmisión de credenciales, tokens, certificados y datos operativos usados por procesos automáticos.	• Transmitir tokens, certificados ni comprobantes por canales HTTP sin cifrado. • Exponer datos de autenticación usados por robots, scripts o agentes inteligentes fuera de un canal cifrado.
Token de acceso y autenticación	• Flujo: Obtener la semilla (GET) → firmarla con un certificado que utilice **SHA-256 o un algoritmo superior** → enviar la semilla firmada (POST) → recibir el token de autenticación, incluyendo los campos **expedido** y **expira**. • Reutilizar el token durante su vigencia (1 hora), renovándolo proactivamente mediante el campo **expira** antes de su vencimiento.	• Solicitar un nuevo token por cada operación individual. • Reintentar la autenticación en bucle sin condición de parada. • Realizar operaciones con token expirado que se traducen en código de respuesta (401). • Permitir que agentes automáticos ejecuten autenticaciones repetitivas sin control, supervisión ni condición de parada.
Certificado digital	• Utilizar certificados digitales emitidos por una de las entidades certificadoras autorizadas por INDOTEL y la DGII para los procesos tributarios. • Monitorear la vigencia del certificado proactivamente,no esperar errores en producción como señal de vencimiento. • Validar el nuevo certificado en pre-certificación antes de activarlo en producción.	• Compartir certificados digitales con terceros. • Obtener token con certificados expirados o revocados. • Emitir comprobantes con certificados expirados o revocados. • Utilizar certificados digitales que no hayan sido emitido por una de las entidades certificadoras autorizadas.

	• Verificar correspondencia RNC-certificado en cada sustitución.	
Conexiones, concurrencia y volumen	• Proporcionalidad: el volumen de conexiones y solicitudes debe ser siempre proporcional al volumen real de operaciones del negocio del contribuyente. • Implementar el uso de conexiones persistentes (Keep-Alive), configurando tiempos de espera (*timeouts*) y límites máximos de conexiones en el pool, así como mecanismos para liberar y cerrar adecuadamente las conexiones que ya no sean necesarias, garantizando una gestión eficiente de los recursos. • Distribuir el envío de forma sostenida para evitar picos abruptos e implementar colas internas. • Proveedores (B2C) con múltiples POS: contemplar el efecto agregado de implementar throttling a nivel de proveedor. • Aplicar límites de concurrencia, tasa y volumen también a automatizaciones, agentes y procesos no interactivos.	• Generar ráfagas de conexiones simultáneas sin justificación operativa. • Concentrar envíos masivos en ventanas horarias cortas. • Establecer múltiples conexiones y dejarlas abiertas, pero sin trazabilidad de operaciones legítimas. • Dimensionar la integración para operar permanentemente al límite sin controles de proporcionalidad. • Escalar concurrencia o volumen artificialmente para compensar deficiencias internas de diseño. • Generar tráfico sostenido que no guarde relación con el volumen real de operaciones del contribuyente.
Envío de comprobantes	• Ante timeout: verificar estado del comprobante antes de cualquier reenvío. Nunca reenviar de forma inmediata. • Usar identificador único de idempotencia por comprobante en todos los reintentos. • Al consultar el estado de un e-CF, validar si el e-NCF fue consumido mediante la propiedad secuenciaUtilizada en los rechazos, cuando su valor sea false, la secuencia puede reutilizarse, y cuando sea true, se debe utilizar la siguiente secuencia disponible. • B2B: registrar el TrackId al enviar. No reenviar mientras la operación original esté pendiente.	• Reenviar de forma inmediata ante timeout sin verificar estado previo del envío original. • Reenviar comprobantes repetidos. • Reutilizar la misma secuencia o reenviar comprobantes sin validar si ya fue consumida. • Omitir el identificador de idempotencia en reintentos del mismo comprobante. • Reenviar una operación B2B mientras el envío original aún se encuentra pendiente de procesamiento.
Consultas de estado (B2B)	• Aplicar backoff progresivo: incrementar el intervalo entre consultas sucesivas sin estado definitivo. • Definir una condición de parada explícita, ya sea por estado definitivo, cantidad máxima de intentos alcanzado o tiempo total acumulado.	• Consultar a alta frecuencia sin espera progresiva (polling agresivo). • Mantener ciclos de consulta indefinidos sin condición de parada. • Consultar reiteradamente el mismo TrackId sin variación de

	• Ante el mismo estado repetido consecutivamente: incrementar el intervalo significativamente y marcar para revisión manual.	intervalo ante ausencia de estado definitivo. • Usar el servicio de consulta como sustituto del control interno de estados del contribuyente. • Mantener consultas automáticas aun cuando el caso ya ha sido procesado, requiere revisión manual o escalamiento técnico.
Errores definitivos de negocio	• No reintentar sin corregir la causa, el mismo comprobante con los mismos datos producirá el mismo rechazo. • Registrar el error con todos sus detalles (código, eNCF, timestamp) y notificar al operador para corrección.	• Reintentar automáticamente comprobantes rechazados por errores definitivos sin corregir la causa del rechazo. • Modificar o reenviar datos de forma improvisada sin trazabilidad ni validación previa. • Descartar, ocultar o no registrar errores definitivos de negocio detectados por la DGII.
Errores de configuración y versión	• Ante error de configuración (certificado vencido, endpoint incorrecto, headers faltantes): detener operaciones y escalar al equipo técnico. • Incluir correctamente el header de versión de API en todas las solicitudes según especificaciones de la DGII. • Ante error de versión no soportada: notificar al equipo técnico y actualizar la integración antes de reintentar.	• Reintentar errores de configuración sin corrección previa. • Confundir certificado vencido con token expirado - son errores de naturaleza distinta. • Operar con endpoints, headers o versiones distintas a las oficialmente soportadas por la DGII. • Ignorar errores de versión no soportada y continuar enviando solicitudes sin actualización previa. • Mantener en producción configuraciones no validadas previamente en el ambiente correspondiente.
Errores transitorios	• Aplicar reintentos con backoff progresivo ante errores o tiempos de espera agotados, estableciendo intervalos de espera y un límite máximo de intentos, evitando incrementar la concurrencia y sobrecargar los servicios.	• Reintentar en bucle o a alta frecuencia sin backoff progresivo ni límite de intentos. • Reenviar comprobantes sin verificar primero si el error fue

	• Verificar el estado del comprobante antes de reenviar - distinguir error de comunicación de error de procesamiento. • Si el error transitorio persiste tras agotar los reintentos: suspender y escalar a revisión manual.	de comunicación o de procesamiento. • Mantener reintentos automáticos aun cuando el error persista, sin suspender ni escalar a revisión manual.
DirectorioFE (B2B)	• Consultar el DirectorioFE como paso previo al envío de un e-CF (B2B) a un comprador electrónico, implementando caché local con un tiempo de vida definido para reducir consultas innecesarias al servicio. • Refrescar el caché ante cambio de estado detectado o al inicio de nueva sesión de trabajo.	• Enviar comprobantes B2B a servicios de receptores que en el directorio electrónico no se encuentran registrados. • Consultar el directorio por cada comprobante individual cuando se procesa una secuencia al mismo receptor. • Cambiar servicios propios sin actualizar oportunamente su registro oficial ante la DGII.

5. Ventanas de Mantenimiento

La DGII publica en tiempo real el estado de disponibilidad de los servicios a través de su canal oficial de monitoreo de estatus. Ante cualquier indisponibilidad, intermitencia o degradación relevante, los contribuyentes deben verificar primero dicho canal antes de ejecutar reintentos o activar procedimientos de contingencia. Cuando los sistemas de la DGII no estén disponibles, los XML o comprobantes generados deberán almacenarse localmente y transmitirse una vez restablecida la comunicación, conforme al Instructivo de Contingencia de Facturación Electrónica.

5.1 Canal oficial de monitoreo de disponibilidad

Portal Estado de Servicios
La publicación del estado en tiempo real de los servicios se realiza en el url:
https://statusecf.dgii.gov.do/help/index.html
Este portal - **FE Estatus Servicios API** - refleja la disponibilidad por servicio y ambiente. Debe ser la primera consulta ante cualquier error de conectividad con el sistema.

5.2 Comportamiento ante indisponibilidad

Cuando los sistemas de la DGII no están disponibles, el contribuyente debe seguir el siguiente procedimiento, conforme al Art. 40 del Decreto 587-24:

- **Generar y firmar los e-CF normalmente** - la emisión no se interrumpe, solo la transmisión.
- **Almacenar los e-CF firmados** en cola local persistente con timestamp, identificador de idempotencia y datos completos.
- Entregar al cliente la Representación Impresa (RI) del e-CF con la leyenda: "e-CF emitido en modalidad de Contingencia, el cual podrá ser consultado para su validez fiscal, a partir de las setenta y dos (72) horas."
- No saturar el sistema en el momento en que comience a responder, el envío de la cola debe ser sostenido, no en ráfaga.

Indisponibilidad prolongada de la DGII
Si la contingencia de la DGII se extiende por más de 15 días hábiles, la Oficina Virtual habilitará la opción para enviar reportes de libros de ventas, compras, gastos, costos y retenciones, operando de manera ordinaria con comprobantes no electrónicos. Mantenga monitoreo del portal de estatus y de las comunicaciones oficiales de la DGII.

5.3 Reanudación controlada tras la restauración

- **Verificar disponibilidad** en el portal statusecf.dgii.gov.do antes de iniciar el envío de la cola acumulada.
- **Transmitir en orden cronológico** y de forma sostenida, no despachar el acumulado en ráfaga. El principio de proporcionalidad aplica también en la fase de recuperación.
- Verificar el estado de los primeros comprobantes enviados antes de continuar, para confirmar que el sistema está procesando correctamente.
- El plazo máximo para transmitir los e-CF generados durante la contingencia por falta de conectividad es de **72 horas** desde el restablecimiento de la comunicación.

6. Procesos de Contingencia del Contribuyente

La contingencia es la situación excepcional o imprevista que impide al contribuyente emitir, transmitir o validar comprobantes fiscales electrónicos (e-CF). El régimen de contingencia está regulado por el **Arts. 40 al 43 del Decreto 587-24**, así como el Art. 21 de la Ley 32-23 y el Art. 10 de la Norma General 01-2020. La DGII ha publicado el Instructivo de Contingencia de Facturación Electrónica como guía oficial de aplicación.

6.1 Tipos de contingencia reconocidos por la DGII

Tipo	Situación	Acciones requeridas
Falta de conectividad	El contribuyente no puede transmitir e-CF por falta de conectividad o intermitencia.	• Generar e-CF offline y transmitir al restablecerse la conexión, en un plazo máximo de 72 horas. • Entregar RI al cliente con la leyenda de contingencia. • No requiere declaración formal en OFV.
Imposibilidad técnica de emitir e-CF	El contribuyente no está en capacidad técnica de emitir e-CF (falla del sistema de facturación, del servidor de firma u otro componente crítico).	• Emitir comprobantes no electrónicos (Serie B) autorizados. • Declarar entrada en contingencia vía Oficina Virtual (OFV). • Declarar salida en OFV al superar la causa.

6.2 Consideraciones normativas clave

Norma / Plazo	Disposición
72 horas (conectividad)	Plazo máximo para transmitir a la DGII los e-CF generados offline por falta de conectividad, una vez restablecida la comunicación.
15 días calendario (imposibilidad)	Duración máxima permitida para la contingencia por imposibilidad técnica de emitir e-CF. (Art. 40, Decreto 587-24)
e-CF sustitutos - solo a la DGII	Los e-CF que reemplazan comprobantes no electrónicos se envían únicamente a la DGII, no al receptor. El receptor sustenta costos con el comprobante ordinario recibido.
Validez fiscal	Solo los comprobantes no electrónicos emitidos en contingencia y correctamente notificados a la DGII son válidos para sustentar costos, gastos y crédito fiscal.
Base legal	Ley 32-23 Art. 21 · Norma 01-2020 Arts. 3(i) y 10 · Decreto 587-24 Arts. 40, 41, 42 y 43

7. Canales de Verificación y Referencias

Nombre	Información
Portal de Estatus	https://statusecf.dgii.gov.do/help/index.html Estado en tiempo real de los servicios eCF, por servicio y ambiente. Debe constituir el primer punto de consulta ante errores de conectividad o indisponibilidad, previo a realizar reintentos o escalamientos. Para su utilización, se requiere gestionar previamente la autorización de acceso correspondiente.
Documentación técnica oficial y normativa vigente del ecosistema e-CF	dgii.gov.do → Facturación → Comprobantes Fiscales Electrónicos (e-CF) Documentación técnica oficial y normativa vigente del ecosistema e-CF.
Contingencia FE - OFV	Oficina Virtual DGII → Facturación Electrónica → Contingencia FE Declaración de entrada y salida de contingencia e histórico de eventos.
Asistencia digital y Telefónica	Canal de atención Telefónica (809) 689-3444 Correo: informacion@dgii.gov.do
Comunidad de Ayuda	Portal web DGII → Comunidad de Ayuda → categoría 'Facturación Electrónica' Base de conocimiento institucional con artículos de ayuda sobre el servicio.
Instructivo Contingencia	dgii.gov.do → Documentación e-CF → Instructivos → Instructivo-Contingencia-FE.

Facturación Electrónica

Centro de Contacto: (809) 689-3444, opción 4
Correo: informacion@dgii.gov.do

En el portal web DGII - Comunidad de Ayuda,

categoría “Facturación Electrónica”

IMPUESTOS INTERNOS
Octubre 2026

Publicación informativa sin validez legal

@DGII