

# Guía Integral para la Integración de Facturación Electrónica del SRI Ecuador en Sistemas de Software (Normativa 2026)

## 1.0 Introducción a la Facturación Electrónica en Ecuador

La facturación electrónica en Ecuador es un sistema digital para la emisión y gestión de comprobantes tributarios, regulado e implementado por el Servicio de Rentas Internas (SRI). Su adopción representa un pilar estratégico para las empresas modernas, ya que reemplaza los documentos tradicionales en papel por archivos electrónicos con plena validez legal. Este sistema garantiza mayor seguridad, transparencia y agilidad en las operaciones comerciales, al tiempo que reduce significativamente los costos operativos asociados a la impresión, envío y almacenamiento de documentos físicos.

El SRI actúa como la autoridad fiscal central que gobierna, valida y autoriza cada transacción dentro de este ecosistema digital. Su rol es asegurar que todos los documentos emitidos cumplan con los estándares técnicos y legales definidos, manteniendo la integridad del sistema tributario nacional.

Los principales tipos de comprobantes electrónicos (*comprobantes electrónicos*) autorizados por el SRI son:

- Factura
- Liquidación de compras de bienes y prestación de servicios
- Nota de crédito
- Nota de débito
- Comprobante de retención
- Guía de remisión

Este sistema, que ha madurado progresivamente, se enfrenta a un cambio regulatorio fundamental programado para 2026, el cual redefinirá las exigencias técnicas para todos los emisores.

## 2.0 El Cambio Normativo Clave para 2026: Transmisión en Tiempo Real

El cambio más crítico en el panorama de la facturación electrónica en Ecuador para el año 2026 es la obligatoriedad de la **transmisión en tiempo real** de todos los comprobantes

electrónicos al SRI. Esta modificación, establecida en la **Resolución NAC-DGERCGC25-00000017**, marca un punto de inflexión en la madurez del sistema tributario digital del país, exigiendo una comunicación instantánea entre los sistemas de facturación de los contribuyentes y la administración tributaria.

A partir del **1 de enero de 2026**, todos los documentos electrónicos deberán ser transmitidos al SRI en el mismo momento en que son generados.

Este nuevo mandato contrasta directamente con el modelo "offline" actual. En el sistema vigente, los contribuyentes disponen de un período de gracia —descrito en la normativa como de hasta 72 horas o cuatro días hábiles— para enviar los comprobantes generados a los servidores del SRI. Este plazo será completamente eliminado.

La supresión de este período de gracia transforma fundamentalmente la arquitectura de los sistemas de software, obligándolos a pasar de un paradigma "orientado a lotes" (batch-oriented) a uno estrictamente "orientado a transacciones" (transaction-oriented). Este cambio impacta todos los niveles del sistema, desde la lógica de confirmación de una venta (commit de base de datos) hasta los bucles de retroalimentación en la interfaz de usuario, exigiendo una arquitectura robusta para garantizar la transmisión inmediata y el cumplimiento fiscal en cada transacción.

## 3.0 Requisitos Fundamentales para Emisores Electrónicos

Antes de iniciar cualquier proceso de integración técnica, las empresas deben cumplir con una serie de prerequisites administrativos y técnicos establecidos por el SRI para obtener la autorización como emisores electrónicos. Estos pasos son indispensables para garantizar que el contribuyente está debidamente habilitado para operar dentro del esquema fiscal digital.

Los requisitos esenciales para que un contribuyente pueda comenzar a emitir comprobantes electrónicos incluyen:

- El contribuyente debe estar registrado en el portal SRI en Línea y poseer credenciales de acceso activas.
- Se debe adquirir y mantener vigente un certificado de firma electrónica, emitido por una entidad de certificación autorizada por el SRI.
- El contribuyente debe solicitar la autorización para emitir comprobantes electrónicos a través del sistema del SRI, un trámite que lo habilita en los ambientes operativos.
- Es obligatorio contar con un software o sistema de facturación que sea capaz de generar los comprobantes en el formato XML requerido por la normativa.
- El emisor debe poseer un convenio de débito registrado y activo en el sistema del SRI.

El SRI ha dispuesto dos ambientes operativos para facilitar el desarrollo y la implementación:

**Ambiente de Pruebas:** Una réplica exacta del sistema de producción, diseñada para que los desarrolladores puedan validar la estructura de los XML, la correcta aplicación de la firma digital y la comunicación con los web services, todo ello sin efectos fiscales reales.

**Ambiente de Producción:** El entorno operativo real donde cada documento transmitido y autorizado tiene plena validez legal y tributaria.

Es crucial entender que la validación exitosa de todos los procesos en el ambiente de pruebas es un requisito obligatorio antes de que el SRI autorice el paso al ambiente de producción. Cumplidos estos prerequisites, se puede proceder con la generación del primer componente técnico clave: el documento XML.

## 4.0 El Proceso de Integración Técnica: Paso a Paso

El ciclo de vida técnico de un comprobante electrónico es una secuencia de pasos precisos e interdependientes que transforman una transacción comercial en un documento fiscalmente válido. Este proceso abarca desde la estructuración de los datos en un formato específico hasta la aplicación de criptografía avanzada y la comunicación con los servicios del SRI para su autorización final.

El flujo técnico completo se puede resumir en los siguientes cinco pasos clave:

1. **Generación del Archivo XML:** Creación del documento estructurado que contiene toda la información de la transacción, siguiendo los esquemas definidos por el SRI.
2. **Generación de la Clave de Acceso:** Construcción de un identificador numérico único de 49 dígitos que sirve como la "cédula de identidad" del comprobante.
3. **Firma Electrónica del XML:** Aplicación de una firma digital bajo el estándar XAdES-BES para garantizar la autenticidad, integridad y no repudio del documento.
4. **Comunicación con los Web Services del SRI:** Envío del documento firmado a los servidores del SRI para su validación y recepción de la respuesta de autorización.
5. **Gestión Post-Autorización:** Generación de la representación impresa (RIDE), entrega al receptor y almacenamiento seguro del XML autorizado a largo plazo.

A continuación, se ofrece un desglose técnico detallado de cada una de estas etapas críticas.

### 4.1 Paso 1: Generación del Archivo XML y la Clave de Acceso

La generación del archivo XML es el punto de partida del proceso. Este archivo debe cumplir con especificaciones técnicas estrictas para ser aceptado por el SRI. La codificación obligatoria es **UTF-8 sin BOM (Byte Order Mark)** para evitar errores de validación. Su estructura se divide en una sección común, **infoTributaria**, que contiene datos del emisor y del documento, y una sección específica según el tipo de comprobante (ej., **infoFactura** para una factura).

Paralelamente, se debe construir la **Clave de Acceso**, un identificador numérico único de 49 dígitos. Esta clave es fundamental, ya que identifica de manera inequívoca cada comprobante en el sistema del SRI. Su composición es la siguiente:

Componente	Descripción	Longitud (dígitos)
<b>Fecha de Emisión</b>	Formato ddmmaaaa	8
<b>Tipo de Comprobante</b>	Código según tabla del SRI (ej. 01 para factura)	2
<b>Número de RUC</b>	RUC del emisor	13
<b>Tipo de Ambiente</b>	1 para Pruebas, 2 para Producción	1
<b>Serie</b>	Código de establecimiento (3) y punto de emisión (3)	6
<b>Número Secuencial</b>	Número del comprobante	9
<b>Código Numérico</b>	Número aleatorio generado por el sistema	8
<b>Tipo de Emisión</b>	1 para Emisión Normal	1
<b>Dígito Verificador</b>	Calculado con el algoritmo Módulo 11	1

El último dígito de la clave se calcula mediante el algoritmo **Módulo 11**. Este procedimiento matemático consiste en multiplicar cada uno de los primeros 48 dígitos por una secuencia de factores (de 2 a 7, de derecha a izquierda), sumar los resultados, obtener el residuo de la división por 11 y restar este valor de 11 para obtener el dígito verificador final. Si el resultado es 11, el dígito es 0; si es 10, el dígito es 1.

## 4.2 Paso 2: Implementación de la Firma Electrónica XAdES-BES

Para garantizar la integridad y autenticidad de los documentos, el SRI exige el estándar de firma **XAdES-BES (XML Advanced Electronic Signatures - Basic Electronic Signature)**

en su variante **"enveloped"**. Esto significa que la estructura de la firma digital se incrusta como un nodo más dentro del propio archivo XML que se está firmando.

La implementación de este estándar desde cero es una tarea de alta complejidad técnica que involucra procesos de normalización (canonicalización), manejo de transformaciones y construcción de estructuras criptográficas precisas. Por ello, se recomienda encarecidamente el uso de bibliotecas especializadas. Para desarrolladores que utilizan el lenguaje Go, una opción validada es **goxades\_sri**, que ha sido específicamente ajustada para cumplir con las particularidades del SRI de Ecuador, como la inclusión de identificadores únicos en los nodos **Signature**, **SignedInfo** y **KeyInfo**.

El proceso técnico de firmado sigue estos pasos:

1. **Carga del Certificado:** Se decodifica el archivo del certificado digital (generalmente un **.p12**) para extraer la clave privada y el certificado público del emisor.
2. **Canonicalización (C14N):** Se normaliza el documento XML para asegurar que variaciones triviales como espacios en blanco o saltos de línea no alteren el hash criptográfico final.
3. **Generación de Digests:** Se calculan los resúmenes criptográficos (usando algoritmos como SHA-256) de los nodos específicos del XML que deben ser protegidos por la firma.
4. **Firma RSA:** El digest resultante se cifra utilizando la clave privada del emisor, creando la firma digital.
5. **Ensamblaje del Nodo **ds:Signature**:** Se construye la estructura completa del nodo de la firma, que contiene los digests, la firma cifrada y el certificado público, y se inserta en el XML original.

#### **Advertencia Crítica:**

Una vez que el documento ha sido firmado, no se debe realizar ninguna modificación, por mínima que sea. Cualquier alteración, incluso cambiar un espacio o un salto de línea, invalidará la firma y causará un rechazo inmediato por parte de los servicios del SRI.

### **4.3 Paso 3: Comunicación con los Web Services SOAP del SRI**

La comunicación entre el software del contribuyente y los servidores del SRI se realiza a través de **Web Services** que utilizan el protocolo **SOAP (versiones 1.1 y 1.2)**. El sistema de facturación debe actuar como un cliente SOAP, capaz de construir y enviar las solicitudes en el formato requerido y procesar las respuestas.

El proceso de comunicación es asíncrono y se divide en dos etapas:

- **Servicio de Recepción:** En este primer paso, el software envía el XML firmado y codificado en Base64. El servicio del SRI realiza validaciones preliminares de estructura y firma. La respuesta puede ser:
  - **RECIBIDA:** El comprobante superó las validaciones iniciales y ha sido encolado para su autorización.

- **DEVUELTA:** El comprobante fue rechazado. La respuesta incluirá un código de error y una descripción del problema (ej., "Firma Inválida", "Esquema XSD no existe").
- **Servicio de Autorización:** Tras obtener una respuesta **RECIBIDA**, se debe consultar este segundo servicio utilizando la **Clave de Acceso** del comprobante. Este servicio devuelve el estado final:
  - **AUTORIZADO:** El comprobante es fiscalmente válido.
  - **NO AUTORIZADO:** El comprobante fue rechazado por motivos de negocio o validaciones más profundas.

A continuación se presentan los puntos de conexión (WSDL) oficiales para ambos ambientes:

Ambiente	Servicio de Recepción	Servicio de Autorización
<b>Pruebas</b>	<a href="https://celcer.sri.gob.ec/comprobantes-electronicos-ws/RecepcionComprobantesOffline?wsdl">https://celcer.sri.gob.ec/comprobantes-electronicos-ws/RecepcionComprobantesOffline?wsdl</a>	<a href="https://celcer.sri.gob.ec/comprobantes-electronicos-ws/AutorizacionComprobantesOffline?wsdl">https://celcer.sri.gob.ec/comprobantes-electronicos-ws/AutorizacionComprobantesOffline?wsdl</a>
<b>Producción</b>	<a href="https://cel.sri.gob.ec/comprobantes-electronicos-ws/RecepcionComprobantesOffline?wsdl">https://cel.sri.gob.ec/comprobantes-electronicos-ws/RecepcionComprobantesOffline?wsdl</a>	<a href="https://cel.sri.gob.ec/comprobantes-electronicos-ws/AutorizacionComprobantesOffline?wsdl">https://cel.sri.gob.ec/comprobantes-electronicos-ws/AutorizacionComprobantesOffline?wsdl</a>

Es fundamental implementar un sistema robusto de manejo de errores que pueda interpretar los códigos devueltos por el SRI. Un sistema bien diseñado debe manejar errores críticos como el **52** ("Error en diferencias") o el **70** ("Clave de acceso en procesamiento"). Este último no debe presentarse como un error inmediato al usuario, sino que requiere una lógica de reintentos asíncronos para consultar el estado del documento posteriormente, demostrando una arquitectura resiliente.

#### 4.4 Paso 4: Gestión Post-Autorización y Almacenamiento

Una vez que un comprobante es autorizado, el proceso no termina. La gestión post-autorización es vital para el cumplimiento legal y la correcta atención al cliente.

El primer componente es el **RIDE (Representación Impresa del Documento Electrónico)**. Este es el formato legible por humanos del comprobante electrónico, comúnmente un archivo PDF. Aunque el documento con validez legal y tributaria es el archivo XML, el RIDE

es esencial para la entrega al cliente, especialmente si este no ha dado su consentimiento para recibir únicamente el formato electrónico o si solicita una copia impresa.

La normativa establece una obligación clara para emisores y receptores: almacenar todos los comprobantes electrónicos (tanto emitidos como recibidos) por un período legal de **7 años**.

Para el almacenamiento, se deben seguir las mejores prácticas. Almacenar miles de archivos XML individuales en una carpeta del sistema de archivos es una práctica deficiente, ya que dificulta la búsqueda, compromete la integridad y no es escalable. La estrategia recomendada es almacenar el contenido del XML y su estado de autorización (**AUTORIZADO, NO AUTORIZADO**) dentro de una **base de datos estructurada** (como SQLite para aplicaciones de escritorio o PostgreSQL para sistemas más robustos). Esta estrategia no solo facilita las auditorías y la generación de reportes, sino que también protege la integridad de los registros fiscales contra la corrupción de archivos o la eliminación accidental, un riesgo inherente al almacenamiento en sistemas de ficheros planos.

## 5.0 Estrategias de Implementación: Desarrollo Nativo vs. APIs de Terceros

Al abordar la integración de la facturación electrónica, las empresas de software se enfrentan a una decisión estratégica fundamental: construir una solución nativa desde cero o integrar un servicio de un proveedor tercero a través de una API. La elección depende de múltiples factores, como el presupuesto disponible, los plazos del proyecto, la experiencia técnica del equipo de desarrollo y el nivel de control deseado sobre el proceso.

A continuación, se presenta una comparación directa de ambos enfoques:

Factor	Desarrollo Nativo	Integración vía API REST
Costo Inicial	Alto (Requiere meses de desarrollo e investigación).	Bajo (La integración se puede completar en días).
Mantenimiento	Requiere dedicación constante para actualizar el sistema ante cambios normativos y técnicos del SRI.	El mantenimiento y las actualizaciones son delegados al proveedor de la API.

<b>Control</b>	Total sobre el flujo del proceso, los datos del cliente y la lógica de negocio.	Dependencia de la disponibilidad, políticas y hoja de ruta del proveedor tercero.
<b>Seguridad de Firma</b>	La firma electrónica y su clave privada residen en la infraestructura del cliente, ofreciendo máximo control.	La firma puede residir en la nube del proveedor, lo que implica delegar la custodia de un activo crítico.
<b>Infraestructura</b>	Requiere únicamente el software cliente instalado y conexión a los servicios del SRI.	Requiere una conexión a internet estable y confiable hacia la API del proveedor.

Para las empresas que prefieren delegar la complejidad técnica, existen varios proveedores en Ecuador que ofrecen APIs robustas. Algunos ejemplos son:

- **Azur Facturación:** Ofrece una API REST que recibe la información de la transacción en formato JSON y gestiona todo el proceso con el SRI. [Más información sobre su API.](#)
- **FacturaSoft:** Proporciona una API REST con autenticación mediante Token Bearer, permitiendo emitir, consultar y gestionar comprobantes electrónicos. [Ver su documentación.](#)

La decisión final debe basarse en un análisis de coste-beneficio que pondere el control y la soberanía de los datos (Desarrollo Nativo) frente a la velocidad de implementación y la reducción de la carga de mantenimiento normativo (API de Terceros).

## 6.0 Conclusión y Recomendaciones Finales

La integración con el sistema de facturación electrónica del SRI es un proyecto de ingeniería de software que exige alta precisión en áreas como la criptografía, la estructuración de datos y la comunicación con protocolos web. El desafío se intensifica con la llegada de la normativa de 2026, que impone la transmisión en tiempo real y elimina cualquier margen para procesos en lote o diferidos. Abordar este reto requiere una planificación meticulosa y un profundo conocimiento técnico de la normativa vigente.

Para asegurar una implementación exitosa y sostenible, se presenta la siguiente hoja de ruta estratégica para mitigar los riesgos de la transición a 2026:

- **Priorizar la Transmisión Inmediata** Diseñar el flujo de trabajo para que el envío del comprobante al SRI sea una parte integral e instantánea del proceso de guardado de la transacción. Se deben evitar los modelos de procesamiento por lotes, ya que no serán compatibles con la nueva normativa.



- **Garantizar la Robustez en el Firmado** Utilizar bibliotecas de firma XAdES-BES que estén validadas y probadas específicamente para el mercado ecuatoriano. Asegurar que la canonicalización del XML sea perfecta es fundamental para evitar rechazos por "Firma Inválida", uno de los errores más comunes.
- **Asegurar los Activos Digitales** Implementar mecanismos de protección robustos para el almacenamiento y uso de los certificados de firma electrónica y sus contraseñas. Estos activos son críticos y su compromiso puede tener graves consecuencias legales y operativas.
- **Educar al Usuario Final** El software debe ser una herramienta que guíe al usuario. Es crucial diseñar interfaces intuitivas que expliquen claramente los estados de los comprobantes, interpreten los errores devueltos por el SRI y faciliten la corrección de datos, minimizando así el riesgo de incumplimiento y posibles sanciones.

En conclusión, un sistema de facturación electrónica bien implementado no es solo una obligación legal, sino una herramienta fundamental que impulsa la eficiencia, la transparencia y la competitividad de las empresas en la economía digital de Ecuador.