Procedimiento de Autorización del Certificador

Contenido

Versión 2.1

1 Certificadores

1.1 Generalidades del certificador

Un certificador es una persona individual, jurídica o entidad no lucrativa que solicita a la Superintendencia de Administración Tributaria, la autorización para realizar la certificación de Documentos Tributarios Electrónicos [1] , establecidos en el Régimen de Factura Electrónica en Línea, de acuerdo a las condiciones siguientes:

a) Una persona individual, jurídica o entidad no lucrativa para prestar el servicio de certificación de documentos a terceros (contribuyentes emisores), o para certificar sus propios documentos, o ambas.

El presente documento reúne todos los requisitos de tipo administrativo, operativo, tecnológico y de seguridad de la información, que las personas jurídicas e individuales deben cumplir para obtener la autorización como certificador. Con el objetivo de garantizar que los certificadores cuenten con experiencia en el ámbito de desarrollo y soporte de sistemas de información, aplicando las mejores prácticas en seguridad de la información que garanticen la continuidad del servicio tanto a sus clientes como a la SAT.

1.2 Pasos para solicitar la autorización como certificador

Para obtener la autorización como certificador, la entidad solicitante debe cumplir con las disposiciones del Régimen de Factura Electrónica en Línea, las leyes tributarias aplicables, y realizar los pasos siguientes:

a) Enviar solicitud escrita a la Intendencia de Recaudación de la SAT, a la dirección:

Departamento de Sistemas de Recaudación
Intendencia de Recaudación
Superintendencia de Administración Tributaria – SAT -
7 avenida 3-73 Zona 9 – Edificio SAT Nivel 7
Ciudad de Guatemala

b) La solicitud debe especificar si se desea autorización para prestar el servicio de certificación a terceros, o bien, si desea autorización únicamente para certificar sus propios documentos.

c) Cumplir con los criterios de autorización incluidos en el presente documento; para ello debe someterse y aprobar la evaluación que la SAT le efectúe.

[1] Ver documento proceso general de Factura Electrónica en Línea

2 Criterios de autorización

2.1 Lista de revisión general del certificador

Lista de revisión general del certificador	
Certificador	
Nombre:	NIT:
Resultado	

¿Cumple con todos los requisitos? *(SÍ o NO)*: …...

¿Puede operar como certificador? *(SÍ o NO)*: …

Fecha de finalización de la verificación: / /

Firma y sello del responsable de la verificación y de su jefe inmediato

Requisitos generales del certificador			
A. **Requisitos administrativos**			
1.	**Solicitud para ser autorizado como certificador**	**¿Cumple?**	
	Solicitud escrita para ser autorizado como certificador de terceros, o bien, si desea autorización únicamente para certificar sus propios documentos. La solicitud debe venir firmada por el representante legal o propietario.		
2.	**Documentos identidad de empresa**	**¿Cumple?**	
	a. Fotocopia de patente de comercio. b. Fotocopia de patente de sociedad c. Fotocopia de escritura de constitución de la sociedad con sus respectivas modificaciones. * Aplica sólo para personas jurídicas. **Para el caso de personas jurídicas no lucrativas**, presentar fotocopia legalizada de la escritura de constitución y sus estatutos debidamente aprobados; adicionalmente, debe presentarse certificación expedida por los registros correspondientes, en la que se haga constar que la entidad cuenta como mínimo con diez (10) años de existencia jurídica.		
3.	**Representante legal o propietario**	**¿Cumple?**	
	a. Fotocopia del nombramiento de representación legal vigente, inscrito en el Registro Tributario Unificado. * b. Fotocopia del Documento Personal de Identificación del representante legal o propietario. *Aplica solo para personas Jurídicas. **Para el caso de personas jurídicas no lucrativas**, la fotocopia del nombramiento debe estar debidamente certificada.		
4.	**Solvencia económica**	**¿Cumple?**	
	Verificar que la empresa cuenta con un capital pagado mínimo de un millón de quetzales. <u>Condiciones para persona jurídica:</u> a. La declaración anual del Impuesto Sobre la Renta (ISR) debe reflejar un capital pagado. b. Si la entidad fue recién creada o su capital fue recién modificado		

	y aún no existe declaración anual de ISR, entonces debe presentar certificación de un contador público y auditor donde conste tener un capital autorizado y pagado mínimo de un millón de quetzales (Q1, 000,000.00) y debe estar asentado en el Registro Mercantil. c. Certificación del libro de Registro de Accionistas donde conste que el capital autorizado está dividido en acciones nominativas y el nombre de los titulares. d. Certificación del Registro Mercantil donde conste que el capital autorizado está dividido en acciones nominativas y el nombre de los titulares. e. Certificación del contador o contador público y auditor del libro de Registro de Accionistas donde conste que el capital autorizado está dividido en acciones nominativas y el nombre de los titulares. <u>Condiciones para persona individual:</u> a. Certificación de un contador público y auditor donde conste tener un capital mínimo de un millón de quetzales (Q1, 000,000.00). ***Condiciones para personas no lucrativas** Certificación contable en la que conste que sus activos fijos netos equivalen como mínimo a un valor de cinco millones de quetzales (Q.5,000,000.00), en el caso de personas jurídicas no lucrativas.		
5.	**Solvencia fiscal**	**¿Cumple?**	
	Presentar solvencia fiscal y SAT verifica que la empresa evidencia un correcto comportamiento tributario. Condiciones: Debe estar actualizado y con estatus activo en el RTU. Debe estar afiliado a los impuestos que correspondan. Debe tener registrado en el RTU como mínimo un representante legal con estatus “activo”. Debe tener registrado en el RTU un contador con estatus “activo”. No debe tener la marca de “no localizado” en el RTU. No debe presentar omisiones en impuestos (IVA, ISR, ISO, e impuestos específicos), ni cuotas atrasadas en convenios de pago. No debe tener expedientes a su nombre en el proceso económico coactivo, (deudas líquidas y exigibles). Las condiciones serán verificadas por medio de los sistemas información de la SAT, de lo cual se adjuntará constancia al expediente de verificación.		
6.	**Declaración jurada**	**¿Cumple?**	
	Verificar que el representante legal del certificador entregue a la SAT una declaración jurada en acta notarial conteniendo el texto siguiente:		

	Bajo juramento declaro que: a. Morosidad: Ni la empresa ni sus representantes legales son deudores morosos del estado. b. Empleados del estado: Ninguno de los accionistas ni representantes legales de la empresa, son empleados de ningún organismo del estado, incluyendo entidades municipales, autónomas, centralizadas y descentralizadas. c. Carencia de sentencia condenatoria: No haber tenido ninguna sentencia por cualquier delito o falta contra el régimen tributario o aduanero en los últimos cinco años. La sentencia mencionada debe haber sido confirmada por un Juez competente en los tribunales de justicia de Guatemala. *En el caso de renovación anual como certificador, presentar vigente. ***Condiciones para personas no lucrativas** Acta de declaración jurada en la que se haga constar que su sistema contable tiene la capacidad de registrar en cuentas separadas los costos y gastos de las rentas afectas y de las rentas exentas, así como que no se deducirán o prorratearan los costos y gastos administrativos que no estén directamente relacionados con la actividad de certificación del Régimen FEL.		
7.	**Personal especializado**	**¿Cumple?**	
	Cuando el certificador preste sus servicios a terceros, debe comprobar que cuenta con los roles y personal especializado. Condiciones: a. Debe existir un gerente o asesor del área tributaria, el cual debe ser profesional de las ciencias económicas, contadores públicos y auditores o ciencias jurídicas y sociales. b. Debe existir un director o gerente del área informática el cual debe ser profesional de ingeniería o ciencias económicas con una carrera orientada al área tecnológica o de sistemas de información. c. Debe contar con un área de auditoría interna o contratar los servicios de auditoría externa. En ambos casos deben ser profesionales contadores públicos y auditores.		
8.	**Solvente en Régimen FACE**	**¿Cumple?**	
	Cuando el solicitante a ser certificador del Régimen FEL haya operado como		

	Generador de Factura Electrónica en el Régimen FACE (Acuerdo de Directorio 024-2007), verificar que no le haya sido rescindido el contrato suscrito con la SAT a petición de la misma y no tenga requerimientos pendientes de resolver.		
9.	**Constancia seminario/taller**	**¿Cumple?**	
	Constancia de participación del personal especializado al seminario/taller "Funcionamiento del Régimen de Factura Electrónica en Línea".		
10.	**Contratos entre el certificador y sus emisores**	**¿Cumple?**	
	Cuando el certificador preste sus servicios a terceros, verificar que el contrato entre él y sus clientes incluye como mínimo las cláusulas siguientes: a. Entrega de los DTE a la SAT. Cláusula en la cual el emisor acepta que el certificador entregue a la SAT la información de los DTE y el certificador se obliga a entregar todos los DTE a la SAT. b. Aceptación de las disposiciones del Régimen de Factura Electrónica en Línea. Cláusula en la cual el emisor se sujeta a las condiciones de emisión de los DTE establecidas por la SAT, incluyendo los requisitos técnicos, la impresión, el almacenamiento y el uso de firmas electrónicas avanzadas como forma de identificación del emisor y certificador, lo que garantiza su autenticidad, integridad, validez y no repudio de los DTE. c. Firma del emisor. Cláusula indicando que cada DTE que el emisor emita y entregue al certificador incluirá una firma electrónica de emisión, a efecto de garantizar la autenticidad, integridad, validez y aceptación de parte del emisor. d. Autenticidad de los DTE. Cláusula en la cual el certificador y el emisor reconocen que los DTE con firma electrónica de emisión válida y certificados son irrefutables para fines legales, judiciales y tributarios respecto de los datos firmados. e. Seguridad de la información. El certificador y el emisor que suscriben el presente contrato del Régimen de Factura Electrónica en Línea, aceptan los requisitos y criterios de seguridad de la información establecidos por la SAT y sus futuras actualizaciones." f. Mesa de ayuda. Cláusula que garantiza que el certificador dispondrá de una mesa de ayuda de acuerdo al horario habitual de facturación del emisor, horario que debe quedar establecido en el contrato. g. Confidencialidad. Cláusula indicando que el certificador se compromete a no divulgar a terceros no autorizados ni a utilizar para fines distintos al Régimen de Factura Electrónica en Línea, la información del emisor a que tenga acceso por la prestación del servicio. h. Relevo de responsabilidad. Cláusula indicando que el certificador es responsable por los servicios de Factura Electrónica en Línea que		

	presta a sus clientes y releva expresamente a la SAT de cualquier obligación que resulte del incumplimiento de los contratos suscritos con los mismos; y cualquier acción u omisión del certificador que cause perjuicio a su emisor, puede derivar en responsabilidad civil y penal.		
11.	**Certificado de seguridad de la información**	**¿Cumple?**	
	Verificar que los procesos que permiten brindar el servicio de certificador, acorde a las disposiciones del Régimen de Factura Electrónica en Línea, cuentan con una de las constancias siguientes: a. Certificado de seguridad de la información vigente, bajo el estándar ISO/IEC 27001 en su versión más reciente. b. Certificado de seguridad de la información emitido por una entidad especializada en seguridad de la información, debidamente autorizada por la SAT para este efecto, en la cual se manifieste que la empresa postulante fue evaluada y cumple con el 100% de los puntos descritos en la matriz de control denominada: Lista de revisión de seguridad del certificador. Dicho certificado debe estar acompañado de la respectiva documentación que evidencie la evaluación realizada satisfactoriamente. El certificado de seguridad debe mantenerse vigente durante todo el tiempo en que se preste el servicio como certificador. La SAT podrá comprobar el cumplimiento de uno o más de los requisitos de seguridad. *En el caso de renovación anual como certificador, presentar vigente.		
12.	**Seguro de caución**	**¿Cumple?**	
	El certificador presenta un seguro de caución emitido por una aseguradora debidamente autorizada para operar en Guatemala por la Superintendencia de Bancos, por un valor de un millón de quetzales (Q1, 000,000.00) a favor de la SAT, para garantizar el cumplimiento de las obligaciones pactadas en el contrato suscrito, por el plazo de un año como mínimo, el cual debe mantenerse vigente mientras dure el contrato entre la SAT y el certificador. *Revisión de renovación		
B. **Requisitos de desempeño**			
1.	**Tiempo de respuesta**	**¿Cumple?**	

	Cuando el certificador preste sus servicios a terceros, verificar que el certificador ofrece al emisor un adecuado tiempo de respuesta por transacción. Condiciones: a. Verificar que la certificación de un DTE que incluya en su detalle 50 ítems de por lo menos 10 caracteres demora 3 segundos o menos. La medición del tiempo inicia desde que el documento llega al certificador hasta que éste certifica el DTE, incluyendo las validaciones y demás procesos intermedios.		
2.	**Mesa de ayuda**	**¿Cumple?**	
	Cuando el certificador preste sus servicios a terceros, verificar que dispone de una mesa de ayuda para sus clientes emisores. Condiciones: a. Debe estar disponible de acuerdo al horario de operación requerido por sus clientes. b. Debe mantener un registro actualizado de las consultas y reclamos de sus emisores.		
3.	**Requerimientos pendientes**	**¿Cumple?**	
	Verificar que el certificador no se encuentre en mora en la entrega a la SAT de ningún requerimiento del Régimen FACE 1 o Factura Electrónica en Línea (por ejemplo, estadísticas, correcciones al sistema, desarrollos de software, etc.)		
4.	**Multas pendientes**	**¿Cumple?**	
	Verificar que el certificador esté solvente en el pago de multas a la SAT, por cualquiera de las faltas establecidas en las disposiciones del Régimen de Factura Electrónica en Línea (sanciones al certificador).		
	C. **Funcionalidad general del sistema del certificador**		
1.	**Registro de emisores**	**¿Cumple?**	
	Cuando el certificador preste sus servicios a terceros, verificar que la aplicación de Factura Electrónica en Línea del certificador cuenta con las funcionalidades mínimas para el registro y control de los emisores. Casos de prueba: a. Registro e historial de los emisores: NIT, nombre, establecimientos, regímenes de afiliación, etc.		
2.	**Servicios disponibles en la SAT**	**¿Cumple?**	

	Verificar que el certificador cuenta con los servicios electrónicos obligatorios establecidos por la SAT en las disposiciones del Régimen de Factura Electrónica en Línea. Casos de prueba: a. Verificar que los servicios estén de alta y funcionan correctamente. b. Verificar que los servicios disponibles por la SAT son consumidos por los sistemas del certificador.		
3.	**Aplicación de validaciones al DTE**	**¿Cumple?**	
	Verificar que el sistema del certificador procese correctamente las validaciones establecidas por la SAT en las disposiciones del Régimen de Factura Electrónica en Línea sobre los diferentes tipos de DTE.		
4.	**Firma del certificador**	**¿Cumple?**	
	Verificar que la llave privada de la firma electrónica del certificador sea custodiada en un módulo de seguridad criptográfico validado bajo el estándar FIPS-140-2 nivel 2 o superior. Caso de prueba: El módulo de seguridad criptográfico se encuentra en la búsqueda oficial provista por NIST. Se brinda evidencia que módulo de seguridad criptográfico es empleado para el sistema.		
5.	**Sincronización de reloj**	**¿Cumple?**	
	Verificar que los servidores utilizados por el sistema del certificador o del servicio que utilice, esté sincronizado con un reloj de alta precisión (GPS o Atómico), un servicio registrado en ntp.org, o bien, el provisto por NIST.		
	D. **Funcionalidad del sistema del certificador para el emisor**		
1.	**Autenticación de usuarios emisor**	**¿Cumple?**	
	Verificar que la aplicación del certificador cuenta con una adecuada plataforma para identificar a los emisores. Casos de prueba: a. Verificar que cuando un emisor ingresa al sistema, se valida su identificador y se le exige por lo menos un factor de autenticación. b. Verificar que existe un mecanismo para que el emisor pueda actualizar el factor de autenticación, por ejemplo, cambio de contraseña, actualización de aplicación o equipo de generación de tokens. c. Verificar que existen pistas de auditoría de accesos y solicitudes de emisión o certificación de DTE.		

2.	**Emisión de documentos**	**¿Cumple?**	
	Cuando el certificador ofrece software o servicio para la emisión de documentos, verificar que la aplicación del certificador cuenta con las funcionalidades mínimas para realizar correctamente las transacciones de emisión de DTE, de acuerdo a los usuarios y perfiles implementados por el certificador. Casos de prueba: a. Emitir documentos de cada tipo de acuerdo a los datos que sean provistos por la SAT. b. Validar y certificar los documentos. c. Enviar a SAT los documentos. d. Almacenar los DTE y sus acuses de recibo. e. Anular DTE.		
3.	**Representación gráfica**	**¿Cumple?**	
	Verificar que el certificador cumple con proveer la representación gráfica del DTE con lo establecido por la SAT. Casos de prueba: a. Verificar que se incluyen los datos mínimos establecidos por la SAT para cada tipo de DTE. b. El tipo de DTE, el identificador único del DTE (número de autorización), los datos del vendedor y los datos del comprador deben quedar claramente consignados en la parte superior. c. Debe ser legible a simple vista, de acuerdo al tamaño y tipo de papel que se seleccione. d. En el caso de los DTE que incluyen complementos, se deben imprimir los datos que correspondan a dichos complementos. e. Incluir las “frases” según corresponda. f. Disponible en formato PDF. g. Si se incluye el QR, éste debe incluir el contenido que establezca la SAT. h. Verificar que coinciden con los datos de los respectivos DTE (archivo XML). i. Si el DTE está anulado, se debe agregar un texto que identifique ese estado.		
4.	**Entrega de DTE al emisor**	**¿Cumple?**	
	Verificar que el sistema del certificador cuenta con servicios de entrega del DTE al emisor por ejemplo correo electrónico, servicios web u otro mecanismo electrónico.		
5.	**Casos de prueba normativos**	**¿Cumple?**	
	Aprobar satisfactoriamente los casos de prueba normativos que la SAT aplique		

	en el ambiente de pruebas del sistema del certificador.		
	E. **Requisitos de tecnología**		
1.	**Arquitectura de la aplicación**	**¿Cumple?**	
	Verificar que la aplicación esté soportada por una arquitectura que permita la escalabilidad, tolerante a fallos y esté implementada con tecnología actual. Casos de prueba: a. Este requerimiento debe ser demostrado con documentación técnica que el certificador debe presentar. b. La SAT se reserva el derecho de realizar pruebas de estrés.		
2.	**Nivel de servicio**	**¿Cumple?**	
	Cuando se trate de una renovación, verificar que el certificador brinda un adecuado nivel de servicio. Casos de prueba: a. Disponibilidad: verificar que los servicios de emisión, certificación, anulación y consulta de DTE del certificador brinda una disponibilidad igual o mayor al 99.7%. Este requerimiento debe ser evidenciado con el reporte anual de incidencias del certificador. Así mismo se podrá confrontar la información con los registros de la SAT derivados de los controles al certificador que para el efecto se establezcan.		
3.	**Documentación técnica del sistema**	**¿Cumple?**	
	Verificar que el certificador cuenta con documentación técnica de la infraestructura informática y de la aplicación utilizada para brindar el servicio de certificador.		
4.	**Archivos XML**	**¿Cumple?**	

	Verificar que los archivos XML de los DTE almacenados por el certificador cumplen con los requisitos establecidos por la SAT en las disposiciones del Régimen FEL y su documentación técnica. Casos de prueba: a. Que estén almacenados de acuerdo al esquema y con firmas válidas. b. Debe demostrarse los controles de seguridad de acceso a la base de datos o almacenamiento de objetos que contienen los archivos XML.		
5.	**Verificar el sistema en producción**	**¿Cumple?**	
	Verificar que el sistema del certificador funciona correctamente. Casos de prueba: a. Registrarse como emisor en su propio sistema informático de certificación de DTE y obtener la autorización de un DTE. b. Emitir y certificar por lo menos dos de cada uno de los tipos de DTE utilizando los NIT que la SAT establece para pruebas. c. Realizar la anulación de uno de los DTE de tipo factura. d. Generar la representación impresa en formato PDF para todos los documentos certificados. e. Obtener acuse de recibo sin errores de la SAT para todos los casos. Casos de prueba: a. Registro e historial de los emisores: NIT, nombre, establecimientos, regímenes de afiliación, etc. *Aplica solo para los certificadores que ya operan como tal.		
6.	**Centros de datos permitidos**	**¿Cumple?**	

	El certificador puede emplear centros de datos propios, servicios de colocación de terceros y servicios en la nube siempre que cumplan para cada caso las condiciones de seguridad desarrolladas más adelante. Casos de prueba: a. Se aceptarán servicios en la nube que operen cumpliendo con certificaciones de seguridad desarrolladas en la lista. b. Se aceptarán servicios de colocación que cuenten con certificaciones de seguridad desarrolladas en la lista. c. Se aceptarán centros de datos propios que hayan sido auditados respecto al cumplimiento de los requisitos de seguridad de centros de datos. d. En el caso de entidades que forman parte de un grupo corporativo, se tomarán como propios centros de datos comunes al grupo corporativo. La SAT se reserva el derecho de calificar este extremo. En relación al punto a y b los requisitos están descritos en el apartado Condiciones para servicios en la nube de la “Lista de revisión de seguridad del certificador”.

2.2 Lista de revisión de seguridad del Certificador

Lista de revisión de seguridad del certificador	
Entidad auditora de seguridad de la información	
Nombre:	NIT:
Certificador	
Nombre:	NIT:
Resultado de la verificación	
¿Cumple el certificador con todos los requisitos que aplican de esta Lista de Revisión? *(ingrese SÍ o NO)***:…** ☐	
Fecha de finalización de la verificación:_____/_____/_____	

Requisitos a verificar por la entidad auditora de seguridad de la información:

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
	Segmentación lógica de infraestructura		
1.	**Segmentación lógica de la red.** La segmentación de la red debe establecerse de acuerdo a la sensibilidad o criticidad de los activos.		
2.	**Filtrado de tráfico entre los segmentos de red.** Únicamente debe habilitarse la comunicación necesaria y autorizada entre las redes virtuales (tipo VLAN (Red de Área Local Virtual del inglés Virtual Local Área Network) o segmentación de redes para servicios en la nube (VPC, por ejemplo).		
3.	**Separación de redes públicas y privadas.** Debe existir por lo menos una DMZ (Zona Desmilitarizada, del inglés Demilitarized Zone) o una forma de separar los servidores públicos de los privados.		
4.	**Separación de ambientes de producción.** Debe existir una separación lógica de los ambientes de producción de otros ambientes, como pruebas o desarrollo.		
	Protección perimetral		
5.	**Protección perimetral por medio de firewall.** Debe estar configurada la protección de los equipos con reglas específicas y denegación de tráfico por defecto, por medio de un firewall en el caso de centros de datos y colocación, o bien, por servicios con capacidades de protección tipo firewall debidamente documentadas por el prestador de servicio.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
6.	**Protección de enlaces o conexiones hacia clientes.** Los enlaces o conexiones hacia clientes deben también estar protegidos por medio de firewall, no se pueden considerar conexiones internas.		
7.	**Debe contar con sistemas de protección de intrusos.** La conexión a Internet debe estar protegida por equipos o servicios con capacidades IDS/IPS.		
8.	**Reglas de protección perimetral seguras.** Las reglas de protección perimetral deben estar documentadas, atender principios de mínimo acceso, únicamente para protocolos seguros. Por ejemplo, no deben existir reglas de “allow all” en la protección perimetral.		
9.	**Protección de navegación contra código malicioso.** El equipo que protege el perímetro de estaciones de trabajo debe contar con protección contra código malicioso.		
10.	**Protección de firewall de aplicaciones.** Los servicios y aplicaciones expuestas a Internet deben contar con firewall de aplicaciones (tipo WAF)		
11.	**Protección contra denegación de servicio.** El acceso por Internet a los servicios y aplicaciones debe contar con protección contra ataques de DoS y DDoS.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
12.	**Alta disponibilidad de protección perimetral.** Debe contar con infraestructura redundante o servicios con alta disponibilidad garantizada en los componentes de seguridad perimetral que garantice el tiempo de disponibilidad requerido.		
13.	**Inventario de servicios expuestos a terceros.** Debe contar con un inventario de servicios/puertos expuestos a terceros.		
14.	**Restricción de servicios no identificados.** Deben existir reglas específicas que apliquen restricciones a puertos no autorizados en el inventario de servicios.		
	Controles de acceso lógico		
15.	**Política de control de accesos.** Para el acceso a activos informáticos e información debe existir una política basada en el acceso mínimo necesario, a nivel de aplicaciones, redes, servidores y bases de datos.		
16.	**Controles de acceso.** Deben existir y se cumplen los controles que refuerzan la política de acceso mínimo necesario, incluyendo la supervisión respecto de los accesos otorgados a nivel de aplicaciones redes, servidores y bases de datos.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
17.	**Política y controles de administración de usuarios.** Debe existir una política de administración de usuarios, se monitorea y cumplen los controles de administración de usuarios que consideren buenas prácticas de seguridad. Se debe contar con matriz de accesos para la administración del sistema y para usuarios del sistema FEL.		
18.	**Política de separación de funciones.** Debe existir una definición de roles y perfiles de acceso de acuerdo a las políticas de acceso y considerando la segregación de funciones del personal y protección de accesos con altos privilegios. Cuando se prestará servicios a terceros, el personal de desarrollo del sistema debe ser distinto al personal responsable de la operación de los ambientes de producción; cuando certificará únicamente sus propios documentos, este control se recomienda, pero no se requiere.		
	Procedimientos de respaldo		
19.	**Ejecución de respaldos automatizados** Debe existir un sistema de respaldos automatizado de toda la información del sistema, en particular las transacciones y documentos emitidos y certificados, así como las bitácoras del sistema.		
20.	**Respaldos completos del sistema.** Debe realizarse un respaldo completo de todos los componentes requeridos para la operación del sistema que permita la recuperación en caso de desastre.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
21.	**Protección y resguardo de los respaldos.** Debe existir una copia redundante electrónica diaria de todas las transacciones de la base de datos en un lugar físico alterno, o bien, por medio de servicios en la nube con durabilidad superior a 99.9999%. (considerando los aspectos de confidencialidad, integridad y disponibilidad de la información).		
22.	**Procedimientos de respaldo y recuperación.** Deben existir procedimientos documentados de los respaldos y recuperación, que incluyan la ejecución de pruebas de restauración periódicas.		
23.	**Control de respaldos.** Deben existir controles documentados de la realización de los respaldos		
24.	**Bitácoras de respaldos.** Deben existir bitácoras de los respaldos realizados.		
25.	**Control de pruebas de recuperación.** Se deben realizar pruebas periódicas de restauración de la información respaldada.		
26.	**Procedimientos de recuperación en caso de falla.** Deben existir procesos documentados de cómo atender fallas de componentes críticos, por ejemplo, la caída de servidores, enlaces, sistemas de comunicación. Presentar planes de contingencia en caso de falla y recuperación en caso de desastre.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
27.	**Traslado de respaldos de sistema.** Debe existir un procedimiento de traslado periódico de respaldos de componentes del sistema hacia un lugar físico alterno (considerando los aspectos de confidencialidad, integridad y disponibilidad de la información).		
28.	**Retención de los respaldos.** La retención de los respaldos de información debe estar de acuerdo al Régimen de Factura Electrónica en Línea. Es decir, debe tener como plazo mínimo 14 meses y extenderse hasta que la SAT indique que se han conciliado los DTE certificados. La retención de los respaldos de sistema para recuperación en caso de desastre deberá atender los planes de recuperación en caso de desastre.		
29.	**Verificación de restauración de información.** La ejecución de la prueba de restauración del último respaldo de la información en un ambiente diferente al de operación debe ser exitosa.		
	Comunicación segura y firma electrónica		
30.	**Comunicación segura.** Toda transmisión de datos entre el certificador y la SAT debe estar encriptada por medio de protocolos seguros.		
31.	**Firma electrónica avanzada.** La firma electrónica de certificación debe realizarse con un certificado de firma emitido por prestador de servicios de certificación autorizado por el RPSC. La firma debe resguardare en un módulo de seguridad criptográfico validado FIPS 140-2 nivel 2 o superior.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
32.	**Política de encripción.** Deben existir políticas y procedimientos documentados sobre la encripción de conexiones, información y almacenamiento sensible		
33.	**Política de gestión de llaves.** Debe existir una, política de gestión adecuada de las llaves de encripción respecto al uso, protección y el tiempo de vida de las llaves criptográficas a través de su ciclo de vida completo		
34.	**Certificados seguros.** La conexión al sistema debe contar como mínimo con una encriptación basada en un certificado SSL de 128 bits o en una clave pública RSA de 2048 bits.		
35.	**Protocolos seguros.** Toda operación del sistema por Internet se debe realizar por protocolos seguros de acuerdo a las mejores prácticas recomendadas por SSL LABS (TLS 1.2 o superiores).		
36.	**Certificados de autoridades reconocidas.** El servidor web y todo servicio web publicado en Internet debe contar con un certificado emitido por una Autoridad Raíz de confianza reconocida.		
37.	**Limitar protocolos inseguros.** No debe existir ninguna transacción del sistema publicada bajo protocolos inseguros (por ejemplo: HTTP o FTP)		
	Segregación de los equipos		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	Observaciones
38.	**Ambiente productivo dedicado.** Los servidores de aplicación y base de datos del ambiente productivo deben ser de uso exclusivo para el sistema de Factura Electrónica en línea. Este criterio debe aplicarse en centros de datos propios y colocación, y en el caso de servicios en la nube, para lo que corresponda al certificador de acuerdo al modelo de responsabilidad compartida de los servicios empleados.		
39.	**Redundancia.** Los servidores de aplicación y base de datos, así como los servicios en la nube que sean empleados deberán contar con, o estar soportados por, esquemas de redundancia.		
40.	**Alta disponibilidad.** La plataforma de almacenamiento debe contar con una configuración que garantice la alta disponibilidad del servicio de acceso a los datos y reduzca los riesgos de pérdida de datos.		
	Documentación de las configuraciones		
41.	**Inventario de activos de hardware y software.** Debe existir documentación por medio de inventarios y control de los componentes de hardware y de software necesarios para la implementación del sistema. Estos inventarios deben considerar los controles recomendados por los controles CIS.		
42.	**Diagramas de red y seguridad perimetral.** Debe existir un mapa (diagrama) actualizado de la red, incluyendo elementos de seguridad perimetral.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
43.	**Diagrama de infraestructura y arquitectura del sistema.** Debe existir un diagrama actualizado de los componentes del sistema, el cual permita identificar sus funciones e interrelaciones. Se recomienda evaluar el uso de diagramas como OBASHI o TOGAF		
44.	**Gestión de cambios.** Debe existir un procedimiento documentado de Gestión de Cambios que se base en un marco de buenas prácticas como ISO-2000, ITIL o MOF. Incluyendo su traslado a producción.		
45.	**Resguardo de la configuración.** Debe existir una copia de la documentación de las configuraciones en un lugar físico alterno (considerando los aspectos de confidencialidad, integridad y disponibilidad de la información).		
	Bitácoras		
46.	**Política de gestión de bitácoras.** Debe existir una política de manejo de bitácoras que contemple el almacenamiento, respaldo, retención, control, monitoreo y auditoría de estas.		
47.	**Bitácoras de auditoria activas.** Las bitácoras de auditoría deben estar activas para todos los sistemas (servidores, bases de datos, entre otros) y dispositivos de red. Estas deben incluir información detallada tales como origen, fecha, usuarios, marca de tiempo, dirección origen, dirección destino y otros elementos de acuerdo al tipo de sistema o dispositivo.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
48.	**Almacenamiento y centralización de logs.** Las bitácoras deben contar con un almacenamiento adecuado y los logs de componentes críticos deben ser incorporados a un sistema central de gestión de logs.		
49.	**Revisión periódica de logs.** Debe realizarse revisiones periódicas de los logs para identificar anomalías y eventos inusuales. Debe planificarse a un año plazo la implementación de una solución tipo SIEM o de análisis y revisión de bitácoras críticas.		
	Políticas de seguridad		
50.	**Políticas de seguridad adecuadas.** Deben existir políticas de seguridad congruentes con buenas prácticas de seguridad, deben estar publicadas y deben ser de conocimiento de las partes interesadas.		
51.	**Uso de contraseñas.** Debe contar con una política de uso de contraseñas, que establezca responsabilidades, controles y requerimientos mínimos de complejidad.		
52.	**Conexión de terceros.** Debe contar con una política de conexión a terceros que incluya bitácora, monitoreo y control.		
53.	**Controles criptográficos.** Debe contar con una política de controles criptográficos que desarrolle los mecanismos de seguridad en la firma de emisión, firma de certificación y los mecanismos de resguardo y custodia de la firma del emisor, si el sistema requiere almacenar el certificado de éste.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	Observaciones
54.	**Política de seguridad de servidores.** Debe implementar protección antimalware y protección tipo firewall en los servidores. Este control deberá ser adecuado conforme al nivel de aseguramiento y riesgo de cada servidor, condición que puede variar derivado de sistemas operativos, prácticas de aseguramiento y acceso a los servidores.		
55.	**Política de seguridad de equipos personales.** Debe implementar encripción de disco, firewall, antimalware en todos los equipos (estaciones de trabajo o portátiles) empleados por personal relacionado con la operación y administración de procesos y sistemas del Régimen FEL. Si se permite el uso de dispositivos móviles, deberá existir una política que aborde los riesgos y establezca controles congruentes con mejores prácticas de seguridad.		
56.	**Política de confidencialidad.** Debe contar con políticas de confidencialidad y privacidad que considere la naturaleza confidencial de los documentos, sea reforzada con controles y del conocimiento de todo su personal, clientes y proveedores.		
57.	**Procedimiento de baja o eliminación de equipos y medios.** Debe contar con un procedimiento que asegure que los equipos y los medios que se eliminen o den de baja eliminen de forma segura toda información confidencial que hayan almacenado.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
	Seguridad de acceso remoto		
58.	**Política de acceso remoto.** En los casos cuando la empresa permita la gestión remota de su infraestructura y plataforma o emplee servicios en la nube, debe existir una política que considere la seguridad de los elementos necesarios, tales como servidores de acceso remoto, múltiple factor de autenticación, canales de comunicación, equipos clientes usados para la conexión, independiente se están en su red o se usan desde cualquier ubicación; esto bajo la premisa que cualquier elemento de comunicación o equipo cliente puede ser sujeto de ataque para procurar acceso al sistema.		
59.	**Solución de acceso remoto.** La solución de acceso remoto que se emplee debe incorporar mecanismo de autenticación y protocolos seguros de comunicación. En ningún caso, se puede permitir la conexión remota directa desde Internet hacia servidores que pertenezcan a segmentos privados. Si caso es gestión de servicios en la nube, deben aplicarse las prácticas de seguridad recomendadas por el proveedor del servicio.		
60.	**Seguridad de los clientes con acceso remoto.** Cualquier equipo cliente que la política permita sea empleada para el acceso remoto debe atender una política de aseguramiento que considere encripción de disco, antimalware, firewall local y política local de seguridad de usuarios y contraseñas. En el caso de dispositivos móviles, capacidad de borrado en caso de pérdida o robo.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
	Controles sobre el personal		
61.	**Selección y reclutamiento.** Debe existir un proceso documentado de selección y reclutamiento, que sea supervisado y verifique la competencia del personal.		
62.	**Revisión del personal.** Se deben revisar y verificar antecedentes e historial laboral de la persona, documentación que debe constar en su expediente laboral.		
63.	**Contratos laborales.** Deben existir contratos laborales firmados que incluyan cláusulas sobre protección de datos, obligación de confidencialidad y no revelación de ningún dato de los clientes y las medidas administrativas, civiles y/o penales que pueden ser aplicadas.		
64.	**Manual de la organización.** Deben existir manuales y descriptores de puestos. En particular deben estar descritas las funciones de gestión de tecnología y sistemas, auditoría interna y atención y asesoría a los emisores.		
65.	**Conciencia de seguridad.** El personal debe ser capacitado y concientizado en las políticas de seguridad de la información de la organización. Debe presentarse evidencia de haber sido realizado para el personal actual, estar incluido en la inducción del personal y contar con una planificación anual.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
66.	**Terminación de contrato.** Deben existir procedimientos documentados para la terminación de la relación laboral, que incorporen los controles y medidas que resguarden la seguridad de usuarios, contraseñas, llave o certificados digitales que hayan sido del conocimiento de quien se retira.		
	Gestión de vulnerabilidades		
67.	**Actualización de seguridad.** Debe contar con política de actualización de parches para todos los componentes del sistema, que refuerce el despliegue de actualizaciones de seguridad.		
68.	**Aseguramiento de componentes.** Debe contar con una política y procedimientos de aseguramiento de componentes, congruente con buenas prácticas y de acuerdo al modelo de responsabilidad que puede aplicar en servicios en la nube.		
69.	**Política de análisis y remediación de vulnerabilidades.** Debe contar con política y procedimientos de evaluaciones y remediaciones de vulnerabilidades. Las evaluaciones deben realizarse como mínimo trimestrales y posterior a cambios significativos en el sistema.		
70.	**Análisis de vulnerabilidades.** Debe tener evidencia de revisiones y mitigación de vulnerabilidades realizadas a los componentes del sistema y en particular a las aplicaciones expuestas a clientes y público.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
71.	**Mitigación de vulnerabilidades.** Debe ser aceptable el nivel de vulnerabilidades detectado o sus medidas de mitigación. Medidas de mitigación en marcha para todas las vulnerabilidades altas (CVSS mayor o igual a 7; del inglés Common Vulnerability Scoring System).		
	Verificación por el auditor		
72.	**Evaluación de vulnerabilidades internas.** Parches de seguridad actualizados en todos los componentes del sistema FEL; endurecimiento de servidores y plataforma, de acuerdo al modelo de responsabilidad compartida cuando se emplean servicios en la nube.		
73.	**Evaluación de vulnerabilidades externas.** Parches actualizados en todos los componentes expuestos al Internet o enlaces con terceros del sistema FEL; endurecimiento de servidores y plataforma, de acuerdo al modelo de responsabilidad compartida cuando se emplean servicios en la nube.		
74.	**Evaluación de vulnerabilidades de las aplicaciones web.** Revisión y mitigación de las vulnerabilidades en las aplicaciones web (este requisito no incluye las denominadas “pruebas de penetración”).		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
	Análisis de riesgo		
75.	**Identificación de activos de información.** Debe contar con un inventario y valoración de los activos críticos relacionados con los procesos del Régimen de Factura Electrónica en Línea, que considere como mínimo las personas, terceros, tecnologías, los servicios en la nube que utilice y cualquier otro componente que pueda suponer un riesgo para la seguridad de la información.		
76.	**Identificación y evaluación de riesgo.** Deben estar plenamente identificadas las amenazas y vulnerabilidades importantes para dichos activos, incluyendo una evaluación del riesgo sobre dichas amenazas y vulnerabilidades. Esta evaluación debe realizarse por lo menos una vez al año.		
77.	**Gestión del riesgo.** Debe existir una política de gestión del riesgo y un plan de tratamiento del riesgo que defina las acciones a tomar respecto a los riesgos residuales que se identificaron. El plan debe contar con aprobación de la Gerencia y ser conocido por el responsable de tecnología y de auditoría interna.		
	Condiciones para proveedores de servicios en la nube **(**Aplicación cuando se emplean servicios de infraestructura y plataforma en la nube)		
78.	**Protección de información en la nube.** El proveedor de nube aplica el código de practica para la protección de información de identificación personal ISO/IEC 27018.		
79.	**Gestión de seguridad del proveedor.** El proveedor de nube cumple con los requisitos de sistemas de gestión de seguridad de la información de la norma ISO/IEC 27001 para lo servicio utilizados.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
80.	**Alianza de seguridad en la nube.** El proveedor de nube se encuentra por lo menos como Self-Assesment en el CSA Security, Trust & Assurance Registry (STAR) .		
81.	**Modelo de responsabilidad compartida.** De acuerdo a los servicios de infraestructura y plataforma contratados, el certificador implementa las políticas y controles adecuado para los componentes y actividades que quedan a su cargo bajo lo modelo de responsabilidad compartida que el proveedor en la nube establece.		
	Condiciones de seguridad para servicios de colocación		
82.	**Contratación de servicios de colocación.** Existe un contrato entre el certificador y el proveedor del servicio que garantice por el plazo de dos años mínimo la prestación del servicio.		
83.	**Capacidad de verificación de seguridad del servicio.** El contrato debe garantizar y deberán ser auditadas de manera independiente todas las condiciones de seguridad del centro de cómputo establecidas y permitir a la SAT y al Auditor de Seguridad, realizar una revisión de estos, o bien, estar respaldado por certificados internacionales, tales como ISO-27001, SOC 2, o Tier 4. La certificación se aceptará como aplicable únicamente para los controles de acceso físico y lógico a los centros de cómputo.		
84.	**Seguridad de los equipos.** Los equipos del certificador deben estar colocados en gabinetes con acceso restringido a terceros.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
	Acceso físico y lógico a centros de cómputo Esta sección aplica para el centro de cómputo que es empleado para el sistema, se exceptúan los servicios de colocación y nube que cuenten con las certificaciones que se consideran válidas		
85.	**Acceso al centro de cómputo.** Deben existir políticas establecidas de control de acceso físico y lógico al centro de cómputo.		
86.	**Responsabilidad de seguridad física.** Dentro de las políticas se debe tener definida la responsabilidad de la seguridad física del centro de cómputo.		
87.	**Procedimientos de autorización.** Debe existir un procedimiento de autorización de acceso al centro de cómputo (incluyendo altas de nuevos usuarios, modificaciones de permisos y bajas de usuarios, ya sea por terminación laboral, cambios de área, ascensos u otros motivos).		
88.	**Bitácora de acceso.** Debe existir un procedimiento de bitácora de acceso al centro de cómputo.		
89.	**Verificación de bitácora.** Deben existir bitácoras de personas autorizadas y personas que ingresan al centro de cómputo.		
90.	**Control por cámara.** Deben existir cámaras que registran el ingreso al centro de cómputo.		
91.	**Controles electrónicos.** Deben existir sensores y controles electrónicos que registren el ingreso al centro de cómputo.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
92.	**Supervisión del acceso.** Debe existir la supervisión de los controles de acceso físico al centro de cómputo por una persona ajena a la administración del centro de cómputo.		
93.	**Resistencia al fuego.** El centro de cómputo debe estar construido con materiales resistentes a las llamas.		
94.	**Protección ante sismos.** El centro de cómputo debe cumplir con regulaciones y protecciones para eventos sísmicos e inundaciones.		
95.	**Perímetro seguro.** Ninguna de las paredes del centro de cómputo debe tener acceso directo a la calle.		
96.	**Acceso al exterior.** El centro de cómputo no debe contar con ventanas que den acceso directo a la calle.		
97.	**Verificación de controles.** Los sistemas de control de acceso deben cumplir con los controles establecidos en la política de acceso.		
98.	**Retención de videos de vigilancia.** Las cámaras de seguridad deben contar con un resguardo de los últimos 3 meses.		
99.	**Protección de acceso.** El centro de cómputo debe contar con alarma antirrobo y de acceso no autorizado.		
100.	**Seguridad de puertas.** Las puertas del centro de cómputo deben ser blindadas y contra incendios.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	Observaciones
101.	**Ambiente adecuado.** El centro de cómputo debe contar con redundancia en los sistemas de aire acondicionado.		
102.	**Tierra física.** El edificio o las instalaciones donde se encuentra el centro de cómputo deben contar con tierra física.		
103.	**Suministro de emergencia.** El centro de cómputo debe contar con un suministro eléctrico de emergencia que garantice la continuidad de las operaciones por un período mínimo de 3 horas.		
104.	**Alimentación redundante.** El centro de cómputo debe contar con alimentación redundante de respaldo, de acuerdo a la carga de equipos que posee.		
105.	**Iluminación de emergencia.** El centro de cómputo debe contar con un sistema de iluminación de emergencia.		
106.	**Protección contra fuego.** El centro de cómputo debe contar con una alarma contra incendios y supresión automática de fuegos.		
107.	**Mantenimiento de equipo.** Los equipos de protección y apoyo (aires acondicionados, UPS, plantas eléctricas, etc.) deben contar con un contrato de mantenimiento preventivo y correctivo.		
108.	**Cableado estructurado.** El centro de cómputo debe contar con una certificación del cableado estructurado.		

	Requisitos de seguridad del certificador	Cumple	
		Si / No / NA	**Observaciones**
109.	**Seguridad de los servidores.** Los servidores y el equipo electrónico deben encontrarse en gabinetes con cerradura.		

2.3 Procedimiento para la autorización del certificador

Luego de que la SAT verifica que la entidad cumple con los "Requisitos para iniciar la operación como certificador" indicados en el párrafo anterior, se procede con lo siguiente:

a) La Intendencia de Recaudación de la SAT emite una Resolución de Autorización del Certificador, la cual especificará si puede prestar el servicio a terceros y/o asimismo.

b) La entidad solicitante firma con la SAT el Contrato administrativo de Certificación de Documentos Tributarios Electrónicos.

c) El Certificador presenta un seguro de caución emitido por una aseguradora debidamente autorizada para operar en Guatemala por la Superintendencia de Bancos, por un valor de un millón de quetzales (Q1,000,000.00) a favor de la SAT, para garantizar el cumplimiento de las obligaciones pactadas en el contrato suscrito, por el plazo de un año como mínimo, el cual debe mantenerse vigente mientras dure el contrato entre la SAT y el certificador.

d) La SAT da de alta al certificador en el sistema de Factura Electrónica en Línea.

e) La SAT verifica el correcto funcionamiento del sistema del certificador en ambiente de producción.

f) La autorización brindada al certificador tiene una vigencia de un año.

2.4 Requisitos para renovar la autorización del certificador

La autorización otorgada al certificador tiene una duración máxima de un año. El certificador es responsable de obtener de la SAT la correspondiente renovación de la autorización.

Para ello, el certificador debe:

a) Continuar cumpliendo con los requisitos que se establecen en las disposiciones del Régimen de Factura Electrónica en Línea como certificador.

b) Aprobar los criterios de Autorización del certificador que la SAT realiza conforme al presente documento.

c) Cumplir con la obligación de enviar a la SAT la totalidad de los DTE que certifique, en las condiciones establecidas en las Disposiciones del Régimen de Factura Electrónica en Línea.

d) Ser emisor de documentos tributarios únicamente bajo el Régimen de Factura Electrónica en Línea.

2.5 Servicios de datos para el certificador

La SAT comparte con los certificadores la información necesaria para que éstos puedan realizar los procesos informáticos propios del Régimen de Factura Electrónica en Línea, siendo la siguiente:

2.5.1 Datos del Registro Tributario Unificado de los emisores de DTE habilitados.
2.5.2 Datos generales de los contribuyentes.
2.5.3 Catálogos para el certificador

Con el objetivo de que los DTE que los certificadores envíen a la SAT cumplan con los estándares establecidos en las Disposiciones del Régimen de Factura Electrónica en Línea y garanticen que son una fuente de información fiable para los procesos propios de la Administración Tributaria, se establecen los catálogos que los emisores deben aplicar al momento de la emisión de documentos y que los certificadores deben validar al momento de la certificación de estos.

La descripción detallada de los mismos estará disponible en el documento denominado “Documento Técnico de Servicios FEL”.

2.6 Características generales del certificador

Debe ser llenado por el certificador, firmado por su Representante Legal y responsables de las áreas de tributos, tecnología y auditoría y entregado en original a la SAT y al Auditor de Seguridad.

Si existen cambios sustanciales en los elementos del perfil, tales como cambio de centros de datos, proveedores de nube o incorporación de nuevos servicios, el Certificador debe notificar a la SAT enviando el perfile actualizado. La SAT se reserva el derecho de requerir una verificación de la auditoría de seguridad.

Instrucciones generales:

- Perfil del certificador.
  Debe completarse con toda la información requerida.
- Oficinas del certificador.
  Debe completarse, con las ubicaciones donde se establezca personal relacionado con los servicios ofrecidos relacionados, por ejemplo, mesa de ayuda, desarrollo y operación del sistema, gestión administrativa de contratos.
- Centros de datos propios.
  Debe ser llenado cuando el certificador emplea centros de datos propios para operación de infraestructura y plataforma del sistema.
- Servicios de colocación.
  Debe ser llenado cuando el certificador emplea servicios de colocación donde opere infraestructura y plataforma del sistema.
- Servicios de infraestructura y plataforma en la nube.
  Debe ser llenado cuando se emplea servicios en la nube.
- Funciones principales del sistema FEL:
  Debe completarse la información para describir las funciones principales ofrecidas por el sistema FEL del certificador:
    - Certificación: Servicio principal obligatorio, debe describir las funciones principales del sistema.
    - Resguardo de DTE por parte del emisor: Características del servicio de resguardo que el certificador puede ofrecer a los emisores, como un servicio adicional al resguardo que como certificador el debe realizar.
    - Firma de emisión: SI el certificador dentro de su plataforma ofrece al emisor la incorporación de la firma de emisión, debiendo describir la forma en que el certificado del emisor es utilizado o resguardado en este proceso.
    - Aplicación o sistema de emisión de DTE: Si el certificador ofrece al emisor una aplicación o sistema que el emisor puede operar para llenar, emitir e incorporar la firma de emisión.

Perfil del certificador			
Certificador			
Nombre del Certificador:		NIT:	
Nombre y firma de responsables[2]			
Representante Legal		NIT:	
Responsable de Auditoría[3]		NIT:	
Responsable de Tecnología		NIT:	
Responsable área de Tributos		NIT	

Oficinas del certificador		
No.	Nombre y Dirección de la oficina	Funciones que se ejecutan
1.		
2.		
3.		

[2] Por responsable, son las personas que reportan directamente a Gerencia en cada área, debe existir por lo menos una, pero podría haber varias por división de funciones. Por ejemplo, responsable de desarrollo de sistemas y un responsable de operación del sistema.

[3] Aclaración: Responsable de la auditoría interna; no se refiere al Auditor de Seguridad

Centros de datos propios		
No.	Nombre y funciones principales	Dirección
1.		
2.		

Servicios de colocación		
No.	Nombre del proveedor	Dirección
1.		
2.		

Servicios en infraestructura y plataforma en la nube		
No.	Nombre del proveedor de servicios en la nube	URL de información de cumplimiento
1.		
2.		

Funciones principales del sistema FEL		
Nombre	SI/NO	Descripción general de funcionalidades
Certificación		
Resguardo de DTE		
Firma de emisión		
Aplicación o sistema de emisión de DTE		