Procedimiento de Autorización del Auditor de Seguridad de la Información

Versión 1

Factura Electrónica en Línea -FEL-

(Acuerdo de Directorio SAT 13-2018)

Julio de 2024

Contenido

1 Entidades Auditoras de Seguridad de la Información

1.1 Objeto

El Acuerdo del Directorio de la SAT No. 13-2018 establece el Régimen de Factura Electrónica en Línea (FEL), y en el presente documento se reúnen los requisitos que las personas jurídicas especialistas en seguridad informática deben cumplir para obtener la autorización como Auditor de Seguridad de la Información.

Las entidades especializadas en evaluación y auditoría de seguridad de la información, pueden solicitar a la SAT, la autorización para evaluar y certificar la seguridad de la información de los Certificadores de Documentos Tributarios Electrónicos del Régimen de Factura Electrónica en Línea. Las entidades extranjeras que deseen participar podrán hacerlo siempre y cuando tengan un representante en la República de Guatemala legalmente constituido para su representación.

La SAT sólo aceptará de los Certificadores de DTE, Certificados de Seguridad de la Información emitidos por entidades que efectivamente hayan obtenido la correspondiente autorización de la SAT, excepto cuando se trate de un Certificado ISO 27001. La auditoría y certificación deberá efectuarse tanto a las entidades que soliciten iniciarse como Certificador, como a las entidades que soliciten continuar como Certificador.

La evaluación que debe realizar el Auditor de Seguridad de la Información implica revisar que el Certificador cumpla con los requisitos establecidos en la “Lista de revisión de seguridad del Certificador”, según el documento “Procedimiento de autorización del certificador” contenido en la Documentación Técnica del Régimen FEL.

1.2 Proceso para autorización

La entidad interesada en ser autorizada como Auditor de Seguridad de la Información, deberá cumplir con lo siguiente:

- Estar actualizado y con estatus activo en el Registro Tributario Unificado.
- Estar afiliado a los impuestos que correspondan.
- Tener registrado en el RTU como mínimo un representante legal con estatus “activo”.
- Tener registrado en el RTU un contador con estatus “activo”.
- No tener la marca de “no localizado” en el RTU.
- No presentar omisiones ni mora en impuestos (IVA, ISR, ISO, e impuestos específicos), ni cuotas atrasadas en convenios de pago.

- No tener expedientes a su nombre en el Proceso Económico Coactivo (deudas líquidas y exigibles).
- No tener ninguna sentencia condenatoria firme por cualquier delito o falta contra el régimen tributario o aduanero en los últimos cinco años.
- Contar con al menos tres (3) años de experiencia en evaluaciones de seguridad de la información en la república de Guatemala y/o en el extranjero.
- Tener dentro de sus empleados a:
    - Al menos un profesional certificado en seguridad de sistemas de información CISSP.
    - Al menos un profesional certificado como Auditor Líder ISO 27001, o bien con certificación CISA.
    - Al menos un técnico o profesional con certificado CEH (del inglés Certified Ethical Hacker)

Presentar solicitud a:

Departamento de Recaudación Tributaria
Intendencia de Recaudación
Superintendencia de Administración Tributaria – SAT –
7ª. Avenida 3-73 Zona 9, Edificio SAT Nivel 7
Ciudad de Guatemala.

1.2.1 Descripción y contenido de la solicitud

i. Carta manifestando su interés en ser autorizada como Auditor de Seguridad de la Información, detallando el nombre de la entidad, el NIT de la entidad, el nombre de la autoridad firmante, teléfono y correo electrónico de la persona de contacto.

ii. Documentos que comprueben que la entidad cuenta con experiencia mínima de tres (3) años en evaluaciones de seguridad de la información en la república de Guatemala y/o en el extranjero.

iii. Hoja de vida del profesional con certificado vigente en seguridad de sistemas de información CISSP (del inglés *Certified Information Systems Security Professional*), debiendo presentar como mínimo copia del certificado antes mencionado y documento de identificación. Los cambios de personal certificado, deberán ser informados a la SAT.

iv. Nombre de un profesional con certificación de Auditor Líder ISO 27001, o bien certificación CISA (del inglés *Certified Information Systems Auditor*), debiendo presentar el currículum correspondiente, los documentos que lo respaldan, tales como título universitario, años de experiencia, copia del certificado antes

mencionado y copia de su DPI. Los cambios de personal certificado, deberán ser informados a la SAT.

v. Nombre de la(s) persona(s) certificada(s) como CEH (del inglés *Certified Ethical Hacker*), debiendo presentar el currículum correspondiente, los documentos que lo respaldan y copia de su DPI. Los cambios de personal certificado, deberán ser informados a la SAT.

vi. Adjuntar el diseño que tendrán los certificados que emitan, debiendo describir las características de seguridad que le permitan a la SAT comprobar su autenticidad. (Ej. hologramas, número de identificación, etc.)

vii. Nombre completo de la(s) persona(s) que firmará(n) los certificados, debiendo adjuntar fotocopia de su DPI.

viii. Especificar un medio electrónico, por el cual la SAT pueda verificar la autenticidad y validez de sus certificados, pudiendo ser cualquiera de estas opciones:

a. Página web con ingreso de parámetros que estén impresos en el certificado.
b. Código de barras QR impreso en el certificado que lleve directamente a la página web donde se confirme su validez.
c. Repositorio donde se aloje la documentación de soporte de la auditoría, incluyendo el certificado, proporcionando a la SAT la dirección (URL) y las credenciales para ingresar.

La información anterior, deberá ser actualizada en la SAT cada vez que sufra cambios, mediante oficio dirigido a donde solicitó su autorización como Auditor de Seguridad de la Información.

1.2.2 Verificación de la SAT

El Departamento de Recaudación Tributaria de la Intendencia de Recaudación atenderá la solicitud recibida y podrá requerir información adicional o realizar investigaciones con terceros si fueran necesarias.

El solicitante debe cumplir a cabalidad con el contenido de la Lista de Revisión para Auditores de Seguridad de la Información.

1.2.3 Autorización de la SAT

Luego de finalizada la verificación de los requisitos, la Intendencia de Recaudación emitirá y enviará electrónicamente a la entidad el aviso de su registro como Auditor de Seguridad de la Información en el Régimen FEL o si el resultado no es favorable, el respectivo aviso denegando la solicitud.

La SAT publicará y mantendrá actualizada en su portal de Internet el registro de entidades autorizadas como Auditores de Seguridad de la Información en el Régimen FEL, incluyendo la información de contacto.

1.2.4 Contratación del certificador a la entidad auditora.

i. Cada Certificador tiene la libertad de elegir la entidad auditora de su preferencia, siempre y cuando esté comprendida en la lista publicada por la SAT.

ii. El costo del servicio de la auditoría y certificación debe ser afrontado en su totalidad por el Certificador. La SAT no pagará ningún servicio ni concepto a la entidad auditora ni al certificador.

1.2.5 Revocación de la autorización de la SAT

La SAT podrá dejar sin efecto en forma permanente la autorización al auditor, por las causales siguientes:

i. Evidencia de que el Auditor no está realizando correctamente las revisiones a los Certificadores que le contratan.
ii. Cambio o ajustes al modelo de operación del Modelo de Factura Electrónica en Línea.
iii. Derogación del Régimen de Factura Electrónica en Línea.
iv. Cualquier otro motivo que convenga a los intereses de la SAT.

En caso de revocación de la autorización a una entidad auditora de seguridad de la información, la SAT podrá revisar y si corresponde, invalidar las certificaciones emitidas por dicha entidad y que se encuentren vigentes. En ese caso el Certificador deberá contratar a otra entidad auditora, para cubrir como mínimo el plazo restante que estaba cubierto por la certificación invalidada. Para cubrir el costo de estas eventuales situaciones, cada vez que el Certificador contrate una entidad certificadora puede exigirle que le entregue un seguro de caución o fianza de garantía.

1.3 Lista de revisión para auditores de seguridad de la información

Lista de revisión para auditores de seguridad de la información		
A) Requisitos Administrativos		
Solvencia tributaria	**¿Cumple?**	
Verificar que la entidad evidencia un correcto comportamiento tributario. Condiciones: a) Debe estar actualizado y con estatus activo en el RTU. b) Debe estar afiliado a los impuestos que correspondan. c) Debe tener registrado en el RTU como mínimo un representante legal con estatus "activo". d) Debe tener registrado en el RTU un contador con estatus "activo". e) No debe tener la marca de "no localizado" en el RTU. f) No debe presentar omisiones ni mora en impuestos (IVA, ISR, ISO, e impuestos específicos), ni cuotasatrasadas en convenios de pago. g) No debe tener expedientes a su nombre en el Proceso Económico Coactivo, (deudas líquidas y exigibles). h) No debe tener ninguna sentencia condenatoria firme por cualquier delito o falta contra el régimen tributarioo aduanero en los últimos cinco años.		
Declaración jurada	**¿Cumple?**	
Verificar que el representante legal del auditor de seguridad de la información entregue a la SATuna Declaración Jurada en acta notarial conteniendo el texto siguiente: "Bajo juramento declaro que: a) Morosidad: Ni la entidad ni sus representantes legales son deudores morosos del Estado. b) Empleados del Estado: Ninguno de los accionistas ni representantes legales de la entidad, son empleados de ningún organismo del Estado, incluyendo entidades municipales, autónomas, centralizadasy descentralizadas.		

Profesionales de seguridad de la información	**¿Cumple?**	
La entidad debe contar como mínimo con tres personas especializadas en seguridad de la información ycubrir las certificaciones siguientes: a) Un profesional universitario con certificado vigente en seguridad de sistemas de información CISSP (delinglés *Certified Information Systems Security Professional*). *b)* Un profesional universitario con certificación de *Auditor Líder ISO 27001*, o bien, certificación *CISA* – *Certified Information Systems Auditor*. *c)* Un técnico o profesional universitario con certificación *CEH – Certified Ethical Hacker.* Debiendo presentar el currículum correspondiente y los documentos que lo respalde, tales como estudios ytítulo universitario (cuando aplica), años de experiencia y copia de cada certificado de los antes mencionados.		
Plantilla o diseño del Certificado que emite y sus medios de verificación	**¿Cumple?**	
• Debe proporcionar copia del diseño que utiliza en los Certificados que emite, y describir todas lascaracterísticas que lo identifican. • Indica el nombre completo de la(s) persona(s) que firmará(n) los certificados y adjunta fotocopia de suDPI. • Especifica algún medio electrónico, por medio del cual la SAT podrá verificar la autenticidad y validezde sus certificados.		

2 Historial de versiones

Versión	Fecha	Ajustes efectuados al presente documento de definición	Autor
1	09/11/2016	Primera versión elaborada como “propuesta”.	David Beltrán
	21/05/2018	Versión final, definición del nombre del actor.	Eduardo Rivera
	10/07/2018	Se suprime el requisito del monto de Capital Pagado.	Eduardo Rivera
	10/07/2018	Se adicionan requisitos relativos a las características ydiseño de los certificados de los interesados.	Eduardo Rivera