RESOLUCIÓN 26930 DE 2000

(Octubre 26)

"Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores"

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

en uso de las facultades legales, en especial las conferidas en los artículos 29, 34, 41 y 42 de la ley 527 de 1999 y los decretos 2153 de 1992, 2269 de 1993 y 1747 de 2000, y

CONSIDERANDO:

En los términos del artículo 41 de la ley 527 de 1999, se faculta a la Superintendencia de Industria y Comercio para autorizar la actividad de las entidades de certificación en el territorio nacional, así como velar por su funcionamiento y la prestación eficiente del servicio.

En el numeral 11 del artículo 41 de la ley 527 de 1999 y en el 21 del artículo 2 del decreto 2153 de 1992, se faculta a la Superintendencia de Industria y Comercio para impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las entidades de certificación.

En el artículo 34 de la ley 527 de 1999 se determina que la Superintendencia de Industria y Comercio autorizará la cesación de actividades de las entidades de certificación.

En el numeral 10 del artículo 2 del decreto 2153 de 1992 y en el numeral 5 del artículo 41 de la ley 527 de 1999, se determina que la Superintendencia de Industria y Comercio podrá solicitar a las personas naturales o jurídicas el suministro de información, datos, informes, libros y papeles de comercio que se requieran para el correcto ejercicio de sus funciones.

Ver art. 34 Ley 527 de 1999
Ver art. 41 Ley 527 de 1999
Ver art. 41 num. 5 Ley 527 de 1999

RESUELVE:

CAPITULO I
Entidades de certificación cerradas

ARTICULO 1°. **Autorización de entidad de certificación cerrada.** La persona que solicite autorización como entidad de certificación cerrada, según lo dispuesto en el numeral 8 del artículo 1 del decreto 1747 de 2000, deberá demostrar el cumplimiento de las condiciones establecidas en el artículo 29 de la ley 527 de 1999 y en los artículos 3 y 4 del decreto 1747 de 2000, para lo cual deberá adjuntar la siguiente información:

1. Certificado de existencia y representación legal, o copia de las normas que le otorgan la calidad de representante legal de una entidad pública o de notario o cónsul.
2. Un formato diligenciado por cada uno de los administradores o representantes legales.

Ver art. 1 num. 8 Decreto Nacional 1747 de 2000

ARTICULO 2°. **Cambio de servicios ofrecidos en entidad de certificación cerrada**. Cuando la entidad de certificación cerrada pretenda ofrecer nuevos servicios como entidad de certificación dentro del entorno cerrado, según lo dispuesto en el numeral 8 del artículo 1 del decreto 1747 de 2000, deberá solicitar autorización previa ante esta Superintendencia.

ARTICULO 3°. **Remisión de información por cambio o actualización de datos en entidad de certificación cerrada**. De conformidad con el artículo 21 del decreto 1747 de 2000, cuando alguno de los datos de la entidad de certificación cerrada que reposan en esta Superintendencia cambie, la entidad de certificación deberá remitir la información correspondiente al cambio, dentro de los 10 días posteriores a la modificación.

En caso de modificación de la información o inclusión de un representante legal o administrador, el nuevo represente legal o administrador deberá diligenciar el *formato* y remitirlo a esta Superintendencia.

ARTICULO 4°. **Información periódica de entidad de certificación cerrada**. La entidad de certificación cerrada deberá almacenar la información de toda su actividad y enviar a esta Superintendencia dentro de los 10 primeros días del inicio de cada trimestre (enero-marzo, abril-junio, julio-septiembre, octubre-diciembre), un archivo de texto, con la siguiente información sobre la actividad del trimestre inmediatamente anterior, discriminada mes a mes:

1. Número de certificados emitidos, de acuerdo con el tipo de certificados.
2. Número de certificados vigentes, de acuerdo con el tipo de certificados.
3. Número de certificados revocados

ARTICULO 5°. **Cesación de actividades en la entidad de certificación cerrada**. Conforme lo dispuesto en el artículo 34 de la ley 527 de 1999 y el artículo 19 del decreto 1747 de 2000, las entidades de certificación cerradas deberán solicitar la autorización de cesación de una o más actividades ante esta superintendencia.

Una vez autorizada la cesación, la entidad de certificación deberá concluir el ejercicio de las actividades autorizadas para cesar, en la forma y siguiendo el cronograma que para el efecto se señale.

ARTICULO 6°. **Publicidad de la entidad de certificación cerrada**. En cualquier publicidad o en cualquier medio en el cual la entidad de certificación ofrezca los servicios deberá indicar que cuenta con autorización de la Superintendencia de Industria y Comercio para operar,
según el siguiente texto : "Entidad de certificación cerrada autorizada por la Superintendencia de Industria y Comercio".

CAPITULO II
Entidades de certificación abiertas

SECCIÓN I
Autorización

ARTICULO 7°. **Autorización de entidad de certificación abierta.** La persona que solicite autorización como entidad de certificación abierta según lo dispuesto en numeral 9 del artículo 1 del decreto 1747 de 2000, deberá demostrar que la actividad está prevista en el objeto social principal, el cumplimiento de las condiciones establecidas en los artículos 29 de la ley 527 de 1999 y 5, 6, 7, 8, 9, 10, 11 del decreto 1747 de 2000 y los estándares, planes y procedimientos de seguridad establecidos en la sección V de esta resolución, adjuntando la siguiente información:

1. *Formato* debidamente diligenciado por cada uno de los administradores o representantes legales adjuntando:

a. Certificado judicial vigente o documento equivalente proveniente del país o países donde haya residido.

b. Copia del certificado de existencia y representación legal, o copia de las normas que le otorgan la calidad de representante legal de una entidad pública o de notario o cónsul.

2. Copia del acto que le otorga la personería jurídica, y copia de las normas que le otorgan la calidad de representante legal de una entidad pública o de notario o cónsul, o certificado de existencia y representación legal. Cuando se trate de persona extranjera se deberá acreditar el cumplimiento de lo señalado en el libro II titulo XIII del código de comercio y el artículo 48 del código de procedimiento civil, según lo dispuesto en el numeral 1 artículo 5 del decreto 1747 de 2000.

3. Informe de auditoría en los términos del artículo 15 de esta resolución.

4. Estados financieros certificados con forme a la ley y con una antigüedad no superior a seis meses, según lo dispuesto en el numeral 1 del artículo 7 del decreto 1747 de 2000.

5. Copia del documento que acredite que se han constituido las garantías de acuerdo a lo dispuesto en el artículo 8 del decreto 1747 de 2000.

6. Documento con descripción detallada de la infraestructura, procedimientos, recursos según lo previsto en el artículo 9 del decreto 1747 de 2000. El cumplimiento de los requisitos deberá acreditarse según lo previsto en la sección V del capítulo II de esta resolución.

En caso de que la infraestructura sea prestada por un tercero, copia de los contratos o convenios con estos, en idioma español.

7. Declaración de prácticas de certificación, en adelante DPC.

SECCIÓN II
Cumplimiento requisitos permanentes

ARTICULO 8°. **Cambio de servicios ofrecidos en entidad de certificación abierta.** Cuando la entidad de certificación abierta pretenda ofrecer nuevos servicios, deberá solicitar autorización previa ante esta Superintendencia, adjuntando el informe de auditoría correspondiente al nuevo servicio.

ARTICULO 9°. **Remisión de información por cambio o actualización de datos en entidad de certificación abierta.** De conformidad con el artículo 21 del decreto 1747 de 2000, cuando

alguno de los datos de la entidad de certificación abierta que reposan en esta Superintendencia cambie, la entidad de certificación deberá remitir la información correspondiente al cambio, dentro de los 10 días posteriores a la modificación.

En caso de modificación de la información o inclusión de un representante legal o administrador, el nuevo represente legal o administrador deberá remitirlo a esta Superintendencia adjuntando:

1. Certificado de Judicial vigente o documento equivalente provenientes del país o países donde haya residido
2. Certificado del órgano competente de los países en que haya residido que certifique que no ha sido excluido o suspendido por actos graves contra la ética de la profesión

ARTICULO 10°. **Información periódica de entidad de certificación abierta**. La entidad de certificación abierta deberá almacenar la información de toda su actividad y enviar a esta Superintendencia dentro de los 10 primeros días del inicio de cada trimestre (enero-marzo, abril-junio, julio-septiembre, octubre-diciembre), un archivo de texto con la siguiente información sobre la actividad del trimestre inmediatamente anterior, discriminada mes a mes:

1. Número de certificados emitidos, de acuerdo con el tipo de certificados.
2. Número de certificados vigentes, de acuerdo con el tipo de certificados.
3. Número de certificados revocados
4. Compromisos adquiridos por cada tipo de certificado.

ARTICULO 11°. **Actualización anual de información de estados financieros, garantías y e informe de auditoría**. La entidad de certificación abierta deberá remitir a esta Superintendencia los estados financieros de fin ejercicio, el informe de auditoría contemplado en el numeral 3 del artículo 7 de esta resolución, dentro de los primeros 15 días corrientes de febrero de cada año calendario.

ARTICULO 12°. **Suspensión programada del servicio**. Durante cada año calendario, las entidades de certificación podrán cesar temporalmente sus actividades por un lapso máximo de 3 días continuos o discontinuos, para mantenimiento del sistema. Cualquier otra suspensión deberá ser solicitada y aprobada por la Superintendencia de Industria y Comercio, previa justificación.

La suspensión permitida deberá informarse a los usuarios con por lo menos con 15 días de antelación y constancia del aviso remitirse a esta Entidad, a mas tardar el primer día de la suspensión.

ARTICULO 13°. **Publicidad de la entidad de certificación abierta**. En cualquier publicidad o en cualquier medio en el cual la entidad de certificación ofrezca los servicios deberá indicar que cuenta con autorización de la Superintendencia de Industria y Comercio para operar,
según el siguiente texto : "Entidad de certificación abierta autorizada por la Superintendencia de Industria y Comercio".

SECCIÓN III
Firmas auditoras de entidades de certificación

ARTICULO 14°. **Firmas auditoras.** La firma auditora nacional que realice el informe de auditoría referido en el artículo 12 del decreto 1747 de 2000, deberá ser un organismo de inspección del sistema nacional de normalización, certificación y metrología acreditada para realizar inspecciones en sistemas informáticos de seguridad y contabilidad, de conformidad con lo señalado en el decreto 2269 de 1993, la resolución 140 de 1994 de la Superintendencia de Industria y Comercio y las disposiciones que los sustituyan o complementen.

Estas firmas deberán cumplir, además de lo requerido en el decreto 2269 de 1993, lo siguiente:

1. Estar compuesta por un grupo interdisciplinario de profesionales que incluirá por lo menos 1 ingeniero de sistemas especializado en sistemas de seguridad, 1 contador y 1 abogado con amplios conocimientos en el tema, quienes deberán cumplir con las normas vigentes relacionadas con cada una de las profesiones.

2. Acreditar experiencia de la firma o de uno de sus socios o funcionarios, en auditorías en sistemas informáticos de seguridad y contabilidad por lo menos de 3 años.

3. Acreditar capacidad para certificar el cumplimiento de los requisitos técnicos y estándares exigidos en la ley 527 de 1999, el decreto 1747 de 2000 y esta resolución.

ARTICULO 15°. **Contenido obligatorio del informe de auditoría**. Tratándose de entidades extranjeras que obren en las condiciones previstas en el artículo 12 del decreto 1747 de 2000, los informes de

auditoría deberán anexar certificación que demuestre que está facultada para realizar este tipo de auditorías en su país de origen.

El informe de auditoria deberá indicar por lo menos:

1. Nombre e identificación de la firma auditora.
2. Fecha de inicio y terminación de la auditoría.
3. Declaración de conformidad de cada una de las condiciones previstas en el artículo 29 de la ley 527 de 1999, el decreto 1747 de 2000, a la presente resolución y las normas que los modifiquen y adicionen.
4. Manifestación de conformidad de la declaración de prácticas de certificación y evaluación de la efectividad de los planes, políticas y procedimientos de seguridad contenidos tanto en la declaración como los exigidos en la sección V de esta resolución.
5. Manifestación del cumplimiento de los estándares indicados en el artículo 23 de esta resolución, teniendo en cuenta criterios reconocidos para el efecto, que cumplan por los menos con los objetivos del nivel de protección 2 (Evaluation Assurance Level 2) definido por Common Criteria for Information Technology Security Evaluation (CC 2.1)CCIMB-99-031 desarrollado por el Common Criteria Project Sponsoring Organization en su parte 3 o su equivalente en la norma ISO/IEC 15408. En el informe deberá precisar para cada uno de estos objetivos del artículo 23 de esta resolución el criterio que observó, la fuente de ese criterio y el reconocimiento que tiene.
6. Firma del representan legal de la firma auditora.

SECCIÓN IV
Cesación de actividades

ARTICULO 16°. **Autorización de cesación de entidades de certificación abiertas** Conforme lo dispuesto en el artículo 34 de la ley 527 de 1999 y el artículo 19 del decreto 1747 de 2000, las entidades de certificación abiertas deberán solicitar autorización de cesación de una o más actividades ante esta Superintendencia, adjuntando la siguiente información:

1. Plan que garantice la protección de la información confidencial de los suscriptores.
2. Plan de conservación de los archivos necesarios para futuras verificaciones de los certificados que emitió, hasta el otorgamiento de la autorización de cesación del servicio. Dicho plan debe permitir el acceso y posterior consulta de los

documentos y extenderse hasta una fecha posterior a la fecha en que se extingan las responsabilidades que se puedan derivar de los certificados expedidos y el plazo que prevean las normas de conservación documental para cada uno de los documentos.

3. Plan que garantice la publicación en los repositorios propios si no cesa todas las actividades o en los de otra entidad de certificación abierta que la Superintendencia de Industria y Comercio determine, si cesará todas las actividades.
4. En caso de cesar todas las actividades de entidad de certificación, un plan de seguridad que garantice la adecuada destrucción de la clave privada de la entidad

ARTICULO 17°. **Procedimiento para la cesación de actividades**. Una vez la Superintendencia autorice la cesación de actividades, la entidad de certificación deberá informar a todos los suscriptores, mediante dos avisos publicados en diarios de amplia circulación nacional, con un intervalo de 15 días, sobre:

1. La terminación de su actividad o actividades y la fecha precisa de cesación.
2. Las consecuencias jurídicas de la cesación respecto de los certificados expedidos.

En todo caso los suscriptores podrán solicitar la revocación y el reembolso equivalente al valor del tiempo de vigencia restante del certificado, si lo solicitan dentro de los dos (2) meses siguientes a la segunda publicación.

La terminación de la actividad o actividades se hará en la forma y siguiendo el cronograma que para el efecto señale la Superintendencia.

SECCIÓN V
Estándares, planes y procedimientos de seguridad

ARTICULO 18°. **Estándares.** Para los efectos previstos en el artículo 27 del decreto 1747 de 2000, admitirán siguientes estándares:

1. **Para algoritmos de firma**.

   a) Algoritmos definidos en el "draft Representation of Public Keys and Digital Signatures in Internet X.509 Public Key Infrastructure Certificates" desarrollado por el PKIX Working group del Internet Engineering Task Force (IETF), excluyendo el MD2.

b) El algoritmo y la longitud de la clave seleccionados deben garantizar la unicidad de la firma digital de los documentos que se firmen de acuerdo con los usos permitidos del certificado. Esta longitud debe ser superior o igual a 1024 bits en el algoritmo de RSA o su equivalente. Longitudes inferiores serán admitidas, pero no menores de 512 bits o su equivalente, previa justificación de garantía de la unicidad.

2. **Para generación de par de claves:** Un método de generación de claves privada y pública que garantice la unicidad y la imposibilidad de estar incurso en situaciones contempladas en el artículo 16 del decreto 1747 de 2000.
3. **Para generación de firma digital**. Un sistema de generación de firma digital que utilice un algoritmo de firma digital admitido.
4. **Para certificados en relación con firma digital**. Los certificados compatibles con el estándar de la International Telecomunication Union (ITU - T) X 509 versión 3.
5. **Para listas de certificados revocados**. El estándar de CRL de la ITU X-509 Versión 2.

ARTICULO 19°. **Declaración de Prácticas de Certificación**. La declaración de prácticas de certificación a que se hace referencia en el artículo 6 del decreto 1747 de 2000, deberá estar accequible desde el "homepage" de la entidad de certificación, disponible al público en todo momento y tendrá que incluir:

1. La identificación de la entidad que presta los servicios de certificación. Esta información incluirá el nombre, razón o denominación social de la entidad, el domicilio social, teléfono, fax, dirección de correo electrónico y la oficina responsable de las peticiones, consultas y reclamos de los suscriptores y usuarios. Si la entidad de certificación tiene entidades subordinadas o subcontratadas, deberá incluir esta misma información respecto de cada una de ellas.
2. La política de manejo de los certificados, que debe incluir:
    a. Los requisitos y el procedimiento de expedición de certificados, incluyendo los procedimientos de identificación del suscriptor y de las entidades reconocidas, de acuerdo con lo previsto en el artículo 43 de la Ley 527 de 1999.
    b. Los tipos de certificados que ofrece, sus diferencias, el grado de confiabilidad y los posibles usos de cada uno de ellos, limites de responsabilidad y el tiempo durante el cual se garantiza la condición de unicidad de la firma digital.

c. El contenido de cada uno de los distintos tipos de certificados.
d. El procedimiento para la actualización de la información contenida en los certificados.
e. El procedimiento, las verificaciones, la oportunidad y las personas que podrán invocar las causales de suspensión o revocación de los certificados.
f. La vigencia de cada uno de los tipos de certificados.
g. La Información sobre el sistema de seguridad para proteger la información que se recoge con el fin de expedir los certificados.

3. Las obligaciones de la entidad de certificación y de los suscriptores del certificado y las precauciones que deben observar los terceros que confían en el certificado.
4. La información que se le va a solicitar a los suscriptores.
5. El manejo de la información que se obtiene de los suscriptores de acuerdo a las normas aplicables en la materia, detallando:
    a. El manejo de la información de naturaleza confidencial.
    b. Los eventos en que se revelará la información confidencial dada por el suscriptor, de acuerdo con las normas vigentes.
6. Las garantías que ofrece la entidad para el cumplimiento de las obligaciones que se deriven de sus actividades y los clausulados de los seguros que protegen a los terceros por los perjuicios que pueda causar la entidad y/o los reglamentos de los contratos de fiducia constituidos para el efecto.
7. Los límites de responsabilidad de la entidad de certificación en cada uno de los tipos de certificados y por cada documento firmado.
8. Las tarifas de expedición y revocación de certificados y los servicios que incluyen.
9. Los procedimientos de seguridad para el manejo de los siguientes eventos:
    a. Cuando la seguridad de la clave privada de la entidad de certificación se ha visto comprometida.
    b. Cuando el sistema de seguridad de la entidad de certificación ha sido vulnerado.
    c. Cuando se presenten fallas en el sistema de la entidad de certificación que comprometan la prestación del servicio.
    d. Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratado por el suscriptor.
10. El plan de contingencia encaminado a garantizar la continuidad del servicio de certificación, en caso de que ocurra algún evento que comprometa la prestación del servicio.

11. Modelos y minutas de los contratos que utilizará. En caso de prever su existencia, texto de las cláusulas compromisorias que establezcan el procedimiento jurídico para la resolución de conflictos, especificando al menos la jurisdicción y ley aplicable en el caso en que alguna de las partes no tenga domicilio en el territorio colombiano.
12. La política de manejo de otros servicios que fuere a prestar, detallando sus condiciones.

ARTICULO 20°. **Sistema confiable**. Para los efectos del artículo 2 del decreto 1747 de 2000 un sistema será confiable cuando cumpla con lo señalado en los artículos 21, 22 y 23 de la presente resolución.

ARTICULO 21°. **Políticas, planes y procedimientos de seguridad**. La entidad debe definir y poner en práctica después de autorizada las políticas, planes y procedimientos de seguridad tendientes a garantizar la prestación continua de los servicios de certificación, que deben ser revisados y actualizados periódicamente. Estos deben incluir al menos:

1. Políticas y procedimientos de seguridad de las instalaciones físicas y los equipos.
2. Políticas de acceso a los sistemas e instalaciones de la entidad, monitoreo constante.
3. Procedimientos de actualización de hardware y software, utilizados para la operación de entidades de certificación.
4. Procedimientos de contingencia en cada uno de los riesgos potenciales que atenten en contra del funcionamiento de la entidad, según estudio que se actualizará periódicamente.
5. Plan de manejo, control y prevención de virus informático.
6. Procedimiento de generación de claves de la entidad de certificación que garantice que:
    a. Solo se hace ante la presencia de los administradores de la entidad.
    b. Los algoritmos utilizados y la longitud de las claves utilizadas son tales que garanticen la unicidad de las firmas generadas en los certificados, por el tiempo de vigencia máximo que duren los mensajes de datos firmados por sus suscriptores.

ARTICULO 22°. **Corta fuegos (Firewall)**. La entidad de certificación debe aislar los servidores de la red interna y externa mediante la instalación de un corta fuegos o firewall, en el cual deben ser configuradas las políticas de acceso y alertas pertinentes.

La red del centro de cómputo debe estar ubicada en segmentos de red físicos independientes de la red interna del sistema, garantizando que el corta fuegos sea el único elemento que permita el acceso lógico a los sistemas de certificación.

ARTICULO 23°. **Sistemas de emisión y administración de certificados**. Los sistemas de emisión y administración de certificados deben prestar en forma segura y continua el servicio. En todo caso las entidades deberán cumplir al menos con una de las siguientes condiciones:

1. Cumplir el Certificate Issuing and Management Components Protection Profile nivel 2 desarrollado por el National Institute of Standards and Technologies; o
2. Cumplir con requerimientos técnicos que correspondan por lo menos con los objetivos del nivel de protección 2 (Evaluation Assurance Level 2) definido por Common Criteria for Information Technology Security Evaluation (CC 2.1) CCIMB-99-031 desarrollado por el Common Criteria Project Sponsoring Organization en su parte 3 o su equivalente en la norma ISO/IEC 15408, de:
    a. Sistema de registro de auditoría de todas las operaciones relativas al funcionamiento y administración de los elementos de emisión y administración de certificados, que permita reconstruir en todo momento cualquier actividad de la entidad;
    b. Sistema de almacenamiento secundario de toda la información de la entidad, en un segundo dispositivo que cuente por lo menos con la misma seguridad que el dispositivo original, para poder reconstruir la información de forma segura en caso necesario;
    c. Dispositivo de generación y almacenamiento de la clave privada, tal que se garantice su privacidad y destrucción en caso de cualquier intento de violación. El dispositivo y los procedimientos deben garantizar que la generación de la clave privada de la entidad solo puede ser generada en presencia de los representantes legales de la misma; y
    d. Sistema de chequeo de integridad de la información sistema, los datos y en particular de sus claves.

CAPITULO III
Certificados

ARTICULO 24°. **Contenido de los certificados.** Los certificados deberán cumplir con lo señalado en el numeral 4 del artículo 18 y con los requisitos exigidos en artículo 35 de la ley 527 de 1999.

ARTICULO 25°. **Contenido de los certificados recíprocos.** Los certificados recíprocos señalados en el parágrafo del artículo 14 del decreto 1747 de 2000 deben contener al menos la siguiente información:

1. Identificador único del certificado.
2. Clave pública de la entidad que se está reconociendo.
3. Tipos de certificados a los que se remite el reconocimiento.
4. Duración del reconocimiento.
5. Referencia de los límites de responsabilidad del tipo de certificado al cual se remite el reconocimiento.

ARTICULO 26°. **Vigencia**. La presente resolución rige a partir de la fecha de su publicación en diario oficial.

PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C. a los

El Superintendente de Industria y Comercio,

EMILIO JOSÉ ARCHILA PEÑALOSA