

DECRETO NUMERO 1747 DE 2000

(septiembre 11)

por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.

El Presidente de la República de Colombia, en ejercicio de las facultades constitucionales y legales, en especial de las conferidas en el numeral 11 del artículo 189 de la Constitución Política y en desarrollo de lo previsto en la Ley 527 de 1999,

DECRETA:

CAPITULO I

Aspectos generales

Artículo 1°. Definiciones. Para efectos del presente decreto se entenderá por:

1. Iniciador: persona que actuando por su cuenta, o en cuyo nombre se haya actuado, envíe o genere un mensaje de datos.

2. Suscriptor: persona a cuyo nombre se expide un certificado.

3. Repositorio: sistema de información utilizado para almacenar y recuperar certificados y otra información relacionada con los mismos.

4. Clave privada: valor o valores numéricos que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.

5. Clave pública: valor o valores numéricos que son utilizados para verificar que una firma digital fue generada con la clave privada del iniciador.

6. Certificado en relación con las firmas digitales: mensaje de datos firmado por la entidad de certificación que identifica, tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la clave pública de éste.

7. Estampado cronológico: mensaje de datos firmado por una entidad de certificación que sirve para verificar que otro mensaje de datos no ha cambiado en un período que comienza en la fecha y hora en que se presta el servicio y termina en la fecha en que la firma del mensaje de datos generado por el prestador del servicio de estampado, pierde validez.

8. Entidad de certificación cerrada: entidad que ofrece servicios propios de las entidades de certificación sólo para el intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello.

9. Entidad de certificación abierta: la que ofrece servicios propios de las entidades de certificación, tales que:

a) Su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, o

b) Recibe remuneración por éstos.

10. Declaración de Prácticas de Certificación (DPC): manifestación de la entidad de certificación sobre las políticas y procedimientos que aplica para la prestación de sus servicios.

Artículo 2°. Sistema confiable. Los sistemas utilizados para el ejercicio de las actividades de certificación se considerarán confiables si satisfacen los estándares establecidos por la Superintendencia de Industria y Comercio.

CAPITULO II

De las entidades de certificación y certificados digitales

Sección I

De las entidades de certificación cerradas

Artículo 3°. Acreditación de requisitos de las entidades de certificación cerradas. Quienes pretendan realizar las actividades propias de las entidades de certificación cerradas deberán acreditar ante la Superintendencia de Industria y Comercio que:

1. Los administradores y representantes legales no están incurso en las causales de inhabilidad previstas en el literal c) del artículo 29 de la Ley 527 de 1999, y
2. Están en capacidad de cumplir los estándares mínimos que fije la Superintendencia de Industria y Comercio de acuerdo a los servicios ofrecidos.

Artículo 4°. Información en certificados. Los certificados emitidos por las entidades de certificación cerradas deberán indicar expresamente que sólo podrán ser usados entre la entidad emisora y el suscriptor. Las entidades deberán informar al suscriptor de manera clara y expresa, previa expedición de los certificados, que éstos no cumplen los requisitos del artículo 15 del presente decreto.

Sección II

De las entidades de certificación abiertas

Artículo 5°. Acreditación de requisitos de las entidades de certificación abiertas. Quienes pretendan realizar las actividades propias de las entidades de certificación abiertas deberán particularizarlas y acreditar ante la Superintendencia de Industria y Comercio:

1. Personería jurídica o condición de notario o cónsul.

Cuando se trate de una entidad extranjera, se deberá acreditar el cumplimiento de los requisitos contemplados en el libro segundo, título VIII del Código de Comercio para las sociedades extranjeras que pretendan ejecutar negocios permanentes en territorio colombiano. Igualmente deberá observarse lo establecido en el artículo 48 del Código de Procedimiento Civil.

2. Que los administradores y representantes legales no están incurso en las causales de inhabilidad previstas en el literal c) del artículo 29 de la Ley 527 de 1999.
3. Declaración de Prácticas de Certificación (DPC) satisfactoria, de acuerdo con los requisitos establecidos por la Superintendencia de Industria y Comercio.
4. Patrimonio mínimo de 400 salarios mínimos mensuales legales vigentes al momento de la autorización.

5. Constitución de las garantías previstas en este decreto.
6. Infraestructura y recursos por lo menos en la forma exigida en el artículo 9° de este decreto.
7. Informe inicial de auditoría satisfactorio a juicio de la misma Superintendencia.
8. Un mecanismo de ejecución inmediata para revocar los certificados digitales expedidos a los suscriptores, a petición de estos o cuando se tenga indicios de que ha ocurrido alguno de los eventos previstos en el artículo 37 de la Ley 527 de 1999.

Parágrafo 1°. La Superintendencia de Industria y Comercio tendrá la facultad de solicitar ampliación o aclaración sobre los puntos que estime conveniente.

Parágrafo 2°. Si se solicita autorización para certificaciones recíprocas, se deberán acreditar adicionalmente la entidad reconocida, los certificados reconocidos y el tipo de certificados al cual se remite, la vigencia y los términos del reconocimiento.

Artículo 6°. Declaración de Prácticas de Certificación (DPC). La Superintendencia de Industria y Comercio definirá el contenido de la Declaración de Prácticas de Certificación, DPC, la cual deberá incluir, al menos lo siguiente:

1. Identificación de la entidad de certificación.
2. Política de manejo de los certificados.
3. Obligaciones de la entidad y de los suscriptores del certificado y precauciones que deben observar los terceros.
4. Manejo de la información suministrada por los suscriptores.
5. Garantías que ofrece para el cumplimiento de las obligaciones que se deriven de sus actividades.
6. Límites de responsabilidad por el ejercicio de su actividad.
7. Tarifas de expedición y revocación de certificados.
8. 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 contratados por el suscriptor.
9. El plan de contingencia encaminado a garantizar la continuidad del servicio de certificación.
10. Modelos y minutas de los contratos que utilizarán con los usuarios.
11. Política de manejo de otros servicios que fuere a prestar, detallando sus condiciones.

Artículo 7°. Patrimonio mínimo. Para determinar el patrimonio mínimo, sólo se tomarán en cuenta las cuentas patrimoniales de capital suscrito y pagado, reserva legal, superávit por prima en colocación de acciones y se deducirán las pérdidas acumuladas y las del ejercicio en curso.

El patrimonio mínimo deberá acreditarse:

1. En el caso de personas jurídicas, por medio de estados financieros, con una antigüedad no superior a 6 meses, certificados por el representante legal y el revisor fiscal si lo hubiere.
2. Tratándose de entidades públicas, por medio del proyecto de gastos y de inversión que generará la actividad de certificación, conjuntamente con los certificados de disponibilidad presupuestal que acrediten la apropiación de recursos para dicho fin.
3. Para las sucursales de entidades extranjeras, por medio del capital asignado.
4. En el caso de los notarios y cónsules, por medio de los recursos dedicados exclusivamente a la actividad de entidad de certificación.

Artículo 8°. Garantías. La entidad debe contar con al menos una de las siguientes garantías:

1. Seguros vigentes que cumplan con los siguientes requisitos:

a) Ser expedidos por una entidad aseguradora autorizada para operar en Colombia. En caso de no ser posible lo anterior, por una entidad aseguradora del exterior que cuente con la autorización previa de la Superintendencia Bancaria;

b) Cubrir todos los perjuicios contractuales y extracontractuales de los suscriptores y terceros de buena fe exenta de culpa derivados de errores y omisiones, o de actos de mala fe de los administradores, representantes legales o empleados de la certificadora en el desarrollo de las actividades para las cuales solicita autorización o cuenta con autorización;

c) Cubrir los anteriores riesgos por una cuantía asegurada por evento igual o superior al mayor entre:

i. 7.500 salarios mínimos mensuales legales por evento; o

ii. El límite de responsabilidad definido en las prácticas de certificación;

d) Incluir cláusula de restitución automática del valor asegurado;

e) Incluir una cláusula que obligue a la entidad aseguradora a informar previamente a la Superintendencia de Industria y Comercio la terminación del contrato o las modificaciones que reduzcan el alcance o monto de la cobertura.

2. Contrato de fiducia con patrimonio autónomo que cumpla con las siguientes características:

a) Tener como objeto exclusivo el cubrimiento de las pérdidas sufridas por los suscriptores y terceros de buena fe exentos de culpa, que se deriven de los errores y omisiones o de actos de mala fe de los administradores, representantes legales o empleados de la certificadora en el desarrollo de las actividades para las cuales solicita o cuenta con autorización;

b) Contar con recursos suficientes para cubrir pérdidas por una cuantía por evento igual o superior al mayor entre:

i. 7.500 salarios mínimos mensuales legales por evento; o

ii. El límite de responsabilidad definido en las prácticas de certificación;

c) Que los fideicomitentes se obliguen a restituir los recursos de la fiducia en caso de una reclamación, por lo menos hasta el monto mínimo exigido en el punto anterior;

d) Que la fiduciaria se obligue a obtener permiso de la Superintendencia de Industria y Comercio, previamente a cualquier cambio en los reglamentos, disminución en el monto o alcance de la cobertura, así como para el retiro de fideicomitentes y para la terminación del contrato;

e) Que las inversiones estén representadas en títulos de renta fija, alta seguridad y liquidez emitidos o garantizados por la Nación, el Banco de la República o calificados como de mínimo riesgo por las sociedades calificadoras de riesgo.

La entidad que pretenda otorgar el reconocimiento recíproco, deberá acreditar la cobertura de las garantías requeridas en este decreto para los perjuicios que puedan causar los certificados reconocidos.

Artículo 9°. Infraestructura y recursos. En desarrollo de lo previsto en el literal b) del artículo 29 de la Ley 527 de 1999, la entidad deberá contar con un equipo de personas, una infraestructura física y tecnológica y unos procedimientos y sistemas de seguridad, tales que:

1. Puedan generar las firmas digitales propias y todos los servicios para los que soliciten autorización.

2. Se garantice el cumplimiento de lo previsto en la Declaración de Prácticas de Certificación (DPC).

3. Se pueda calificar el sistema como confiable de acuerdo con lo señalado en el artículo 2° del presente decreto.

4. Los certificados expedidos por las entidades de certificación cumplan con:

a) Lo previsto en el artículo 35 de la ley 527 de 1999; y

b) Alguno de los estándares de certificados que admita de manera general la Superintendencia de Industria y Comercio.

5. Se garantice la existencia de sistemas de seguridad física en sus instalaciones, un monitoreo permanente de toda su planta física, y acceso restringido a los equipos que manejan los sistemas de operación de la entidad.

6. El manejo de la clave privada de la entidad esté sometido a un procedimiento propio de seguridad que evite el acceso físico o de otra índole a la misma, a personal no autorizado.

7. Cuenten con un registro de todas las transacciones realizadas, que permita identificar el autor de cada una de las operaciones.

8. Los sistemas que cumplan las funciones de certificación sólo sean utilizados con ese propósito y por lo tanto no puedan realizar ninguna otra función.

9. Todos los sistemas que participen directa o indirectamente en la función de certificación estén protegidos por sistemas y procedimientos de autenticación y seguridad de alto nivel de protección, que deben ser actualizados de acuerdo a los avances tecnológicos para garantizar la correcta prestación del servicio.

Artículo 10. Infraestructura prestada por un tercero. Cuando quiera que la entidad de certificación requiera o utilice infraestructura o servicios tecnológicos prestados por un tercero, los contratos deberán prever que la terminación de los mismos está condicionada a que la entidad haya implementado o contratado una infraestructura o servicio tecnológico que le permita continuar prestando sus servicios sin ningún perjuicio para los suscriptores. Si la terminación de dichos contratos supone el cese de operaciones, el prestador de infraestructura o servicios no podrá interrumpir sus servicios antes de vencerse el plazo para concluir el proceso previsto en el procedimiento autorizado por la Superintendencia de Industria y Comercio. Estos deben ser enviados con los demás documentos de la solicitud de autorización y remitidos cada vez que sean modificados.

La contratación de esta infraestructura o servicios no exime a la entidad certificadora de la presentación de los informes de auditoría previstos en este decreto, los cuales deben incluir los sistemas y seguridades de dicho prestador.

Artículo 11. Informe de Auditoría. El informe de Auditoría dictaminará que la entidad de certificación actúa o está en capacidad de actuar, de acuerdo con los requerimientos de la Ley 527 de 1999, lo previsto en este decreto y en las normas que los sustituyan, complementen o reglamenten. Así mismo, evaluará todos los servicios a que hace referencia el literal d del artículo 2° de la Ley 527 de 1999 y que sean prestados o pretenda prestar la entidad de certificación.

Artículo 12. Requisitos de las firmas auditoras. La auditoría deberá ser realizada por una entidad del sistema nacional de normalización, certificación y metrología acreditada para el efecto por la Superintendencia de Industria y Comercio.

En caso de tratarse de entidades de certificación que requieran o utilicen infraestructura o servicios tecnológicos prestados desde el extranjero, la auditoría podrá ser realizada por una persona o entidad facultada para realizar este tipo de auditorías en el lugar donde se encuentra la infraestructura, siempre y cuando permita constatar el cumplimiento de lo señalado en el artículo anterior.

En caso de que no existan en el país al menos dos entidades acreditadas para llevar a cabo estas auditorías, las entidades de certificación nacionales podrán hacer uso de firmas de auditorías extranjeras, siempre y cuando el informe cumpla con las instrucciones impartidas por la Superintendencia de Industria y Comercio y la firma auditora se encuentre facultada para realizar este tipo de auditorías en su país de origen.

Artículo 13. Deberes. Además de lo previsto en el artículo 32 de la Ley 527 de 1999, las entidades de certificación deberán:

1. Comprobar por sí o por medio de una persona diferente que actúe en nombre y por cuenta suya, la identidad y cualesquiera otras circunstancias de los solicitantes o de datos de los certificados, relevantes para los fines propios de su procedimiento de verificación previo a su expedición.
2. Mantener a disposición permanente del público la declaración de prácticas de certificación.
3. Cumplir cabalmente con las políticas de certificación acordadas con el suscriptor y con su Declaración de Prácticas de Certificación (DPC).
4. Informar al suscriptor de los certificados que expide, su nivel de confiabilidad, los límites de responsabilidad, y las obligaciones que el suscriptor asume como usuario del servicio de certificación.

5. Garantizar la prestación permanente e ininterrumpida de los servicios autorizados, salvo las interrupciones que autorice la Superintendencia de Industria y Comercio.
6. Informar a la superintendencia de manera inmediata la ocurrencia de cualquier evento establecido en la Declaración de Prácticas de Certificación, que comprometa la prestación del servicio.
7. Abstenerse de acceder o almacenar la clave privada del suscriptor.
8. Mantener actualizado el registro de los certificados revocados. Las entidades de certificación serán responsables de los perjuicios que se causen a terceros por incumplimiento de esta obligación.
9. Garantizar el acceso permanente y eficiente de los suscriptores y de terceros al repositorio de la entidad.
10. Disponer de una línea telefónica de atención permanente a suscriptores y terceros, que permita las consultas y la pronta solicitud de revocación de certificados por los suscriptores.
11. Garantizar la confidencialidad de la información que no figure en el certificado.
12. Conservar la documentación que respalda los certificados emitidos, por el término previsto en la ley para los papeles de los comerciantes y tomar las medidas necesarias para garantizar la integridad y la confidencialidad que le sean propias.
13. Informar al suscriptor dentro de las 24 horas siguientes, la suspensión del servicio o revocación de sus certificados.
14. Capacitar y advertir a los suscriptores de firmas y certificados digitales, sobre las medidas de seguridad que deben observar para la utilización de estos mecanismos.
15. Mantener el control exclusivo de su clave privada y establecer las seguridades necesarias para que no se divulgue o comprometa.
16. Remitir oportunamente a la Superintendencia de Industria y Comercio, la información prevista en este decreto.
17. Remover en el menor término que el procedimiento legal permita, a los administradores o representantes que resulten incurso en las causales establecidas en el literal c del artículo 29 de la Ley 527 de 1999.
18. Informar a los suscriptores o terceros que lo soliciten, sobre el tiempo y recursos computacionales requeridos para derivar la clave privada a partir de la clave pública contenida en los certificados en relación con las firmas digitales que expide la entidad.
19. Mantener actualizada la información registrada en la solicitud de autorización y enviar la información que la Superintendencia de Industria y Comercio establezca.
20. Cumplir con las demás instrucciones que establezca la Superintendencia de Industria y Comercio.

Artículo 14. Certificaciones recíprocas. El reconocimiento de los certificados de firmas digitales emitidos por entidades de certificación extranjeras, realizado por entidades de certificación autorizadas para tal efecto en Colombia, se hará constar en un certificado expedido por estas últimas.

El efecto del reconocimiento de cada certificado, se limitará a las características propias del tipo de certificado reconocido y por el período de validez del mismo.

Los suscriptores de los certificados reconocidos y los terceros tendrán idénticos derechos que los suscriptores y terceros respecto de los certificados propios de la entidad que hace el reconocimiento.

Parágrafo. La Superintendencia de Industria y Comercio determinará el contenido mínimo de los certificados recíprocos.

Artículo 15. Uso del certificado digital. Cuando quiera que un suscriptor firme digitalmente un mensaje de datos con su clave privada, y la respalde mediante un certificado digital, se darán por satisfechos los atributos exigidos para una firma digital en el parágrafo del artículo 28 de la Ley 527 de 1999, sí:

1. El certificado fue emitido por una entidad de certificación abierta autorizada para ello por la Superintendencia de Industria y Comercio.
2. Dicha firma se puede verificar con la clave pública que se encuentra en el certificado con relación a firmas digitales, emitido por la entidad de certificación.
3. La firma fue emitida dentro del tiempo de validez del certificado, sin que éste haya sido revocado.
4. El mensaje de datos firmado se encuentra dentro de los usos aceptados en la DPC, de acuerdo al tipo de certificado.

Artículo 16. Unicidad de la firma digital. No obstante lo previsto en el artículo anterior, una firma digital en un mensaje de datos deja de ser única a la persona que la usa si, estando bajo su control exclusivo, dada la condición del numeral 3 del parágrafo del artículo 28 de la Ley 527 de 1999, la probabilidad de derivar la clave privada, a partir de la clave pública, no es o deja de ser remota.

Para establecer si la probabilidad es remota se tendrán en cuenta la utilización del máximo recurso computacional disponible al momento de calcular la probabilidad, durante un período igual al que transcurre entre el momento en que se crean el par de claves y aquel en que el documento firmado deja de ser idóneo para generar obligaciones.

Sección III

De la decisión y las responsabilidades

Artículo 17. Decisión. En la resolución de autorización expedida por la Superintendencia de Industria y Comercio, se precisarán las actividades y servicios que puede prestar la entidad de certificación. En todo caso, la entidad de certificación podrá solicitar autorización para prestar actividades y servicios adicionales.

Artículo 18. Responsabilidad. Las entidades de certificación responderán por todos los perjuicios que causen en el ejercicio de sus actividades.

La entidad certificadora será responsable por los perjuicios que puedan causar los prestadores de servicios a que hace referencia del artículo 10 del presente decreto, a los suscriptores o a las personas que confíen en los certificados.

Artículo 19. Cesación de actividades. La cesación de actividades de una entidad de certificación sin la autorización de la Superintendencia de Industria y Comercio o la

continuación de actividades después de producida ésta, la hará responsable de todos los perjuicios que cause a sus suscriptores y a terceros y la hará acreedora a las sanciones que imponga la Superintendencia.

Artículo 20. Responsabilidad derivada de la administración de los repositorios. Cuando las entidades de certificación contraten los servicios de repositorios, continuarán siendo responsables frente a sus suscriptores y terceros por el mismo.

Artículo 21. Información periódica y esporádica. La información prevista en los artículos 3°, 5°, 6°, 7°, 8°, 9°, 10 y 11 del presente decreto, deberá actualizarse ante la Superintendencia de Industria y Comercio cada vez que haya cambio o modificación de algunos de los datos suministrados. La Superintendencia señalará, además, la forma y periodicidad en que se debe demostrar el continuo cumplimiento de las condiciones de que se ocupan los artículos señalados.

Artículo 22. Responsabilidad derivada de la no revocación. Una vez cumplidas las formalidades previstas para la revocación, la entidad será responsable por los perjuicios que cause la no revocación.

Sección IV

De los certificados digitales

Artículo 23. Información relativa a la revocación. Cada certificado revocado debe indicar si el motivo de revocación incluye la pérdida de control de la clave privada, evento en el cual, las firmas generadas con dicha clave privada carecerán del atributo de unicidad previsto en el numeral 1 del párrafo del artículo 28 de la Ley 527 de 1999, salvo que se demuestre lo contrario, mediante un mecanismo adicional que pruebe inequívocamente que el documento fue firmado digitalmente en una fecha previa a la revocación del certificado.

Las revocaciones deberán ser publicadas de manera inmediata en los repositorios correspondientes y notificadas al suscriptor dentro de las 24 horas siguientes. Si dichos repositorios no existen al momento de la publicación del aviso, ésta se efectuará en un repositorio que designe la Superintendencia de Industria y Comercio.

Artículo 24. Registro de certificados. Toda entidad de certificación autorizada deberá llevar un registro de público acceso que contenga todos los certificados emitidos y sus fechas de emisión, expiración o revocación.

Artículo 25. Información. Las entidades de certificación estarán obligadas a respetar las condiciones de confidencialidad y seguridad, de acuerdo con las normas vigentes respectivas.

Salvo la información contenida en el certificado, la suministrada por los suscriptores a las entidades de certificación se considerará privada y confidencial.

CAPITULO III

Facultades de la Superintendencia de Industria y Comercio

Artículo 26. Suspensión y revocación de autorización. Cuando quiera que la Superintendencia de Industria y Comercio ejerza la facultad contenida en el numeral 4 del artículo 41 de la Ley 527 de 1999, ordenará a la entidad de certificación la ejecución de medidas tendientes a garantizar la integridad, seguridad y conservación de los certificados expedidos, así como la compensación económica que pudiera generar la cesación de actividades.

Artículo 27. Estándares. La Superintendencia de Industria y Comercio determinará los estándares admisibles con respecto a los cuales las entidades - de certificación deberán acreditar el cumplimiento de los requisitos relativos a:

1. La generación de pares de claves.
2. La generación de firmas.
3. Los certificados.
4. Los sistemas de cifrado.
5. Las comunicaciones.
6. La seguridad de los sistemas de información y de las instalaciones, o
7. Cualquier otro aspecto que redunde en la confiabilidad y seguridad de los certificados, o de la información que repose en la entidad de certificación.

Para la determinación de los estándares admisibles, la superintendencia deberá adoptar aquellos que tengan carácter internacional y que estén vigentes tecnológicamente o los desarrollados por el organismo nacional de normalización o los que sean ampliamente reconocidos para los propósitos perseguidos. En todo caso, deberá tener en cuenta su aplicabilidad a la luz de la legislación vigente.

La Superintendencia podrá eliminar la admisibilidad de un estándar cuando haya dejado de cumplir alguno de los requisitos precisados en este artículo.

Artículo 28. Facultades. Las atribuciones otorgadas a la Superintendencia de Industria y Comercio en el presente decreto, se ejercerán conforme a las facultades establecidas en los artículos 41 de la Ley 527 de 1999 y en los Decretos 2269 de 1993 y 2153 de 1992.

Artículo 29. Vigencia. El presente decreto rige a partir de la fecha de su publicación y deroga las disposiciones que le sean contrarias.

Publíquese y cúmplase.

Dado en Bogotá, D. C., a 11 de septiembre de 2000.

ANDRES PASTRANA ARANGO

El Ministro de Desarrollo Económico,

Augusto Ramírez Ocampo.

La Ministra de Comercio Exterior,

Marta Lucía Ramírez de Rincón.

La Ministra de Comunicaciones,

María del Rosario Sintés Ulloa.