



## TÍTULO I DISPOSICIONES GENERALES

En este primer título se encuentran las instrucciones que tienen como destino dos o más entidades o sujetos de vigilancia y aquellas relacionadas con las nuevas facultades jurisdiccionales y de conciliación otorgadas a la Superintendencia.

### CAPÍTULO PRIMERO

#### **SEGURIDAD TÉCNICA Y JURÍDICA PARA LAS COMUNICACIONES ELECTRÓNICAS DE LA SUPERINTENDENCIA NACIONAL DE SALUD QUE REQUIEREN FIRMA DIGITAL.**

Con el fin de garantizar un intercambio seguro y eficiente de los datos entre los vigilados y la entidad, y garantizar los atributos de autenticidad, integridad y no repudio de la información, la Superintendencia Nacional de Salud, incorpora la aplicación de nuevas tecnologías de seguridad en sus comunicaciones electrónicas, de conformidad con lo establecido en la ley 527 de 1999, el decreto reglamentario 1747 de 2000; que definen y reglamentan el acceso y uso de los mensajes de datos, así como la firma digital y las entidades de certificación.

En particular, se busca, entre otros objetivos, reducir al mínimo posible la utilización y flujo de documentos en soporte caratular (papel), asegurando la identificación plena de los emisores de documentos electrónicos, certificando la recepción efectiva y oportuna de los datos por parte del verdadero destinatario y garantizando la seguridad técnica y jurídica (dado su valor probatorio) de la información. Dicha seguridad en los entornos electrónicos se refleja en atributos jurídicos como la autenticidad, integridad y no repudio.

El sistema de certificación digital permite establecer la identidad y otras cualidades de una persona que actúa a través de una red informática, un sistema de información y, en general, cualquier medio de comunicación y/o información electrónica. De esta forma, la certificación digital garantiza: la identificación y capacidad de las partes que tratan entre sí sin conocerse (emisor y receptor del mensaje); la confidencialidad de los contenidos de los mensajes (ni leídos, ni escuchados por terceros); la integridad de la transacción (no manipulada por terceros) y la irrefutabilidad de los compromisos adquiridos (no repudiación).



Teniendo en cuenta lo anterior, los archivos reportados a la Superintendencia vía electrónica deberán llegar debidamente autenticados, a través de la utilización de firma digital. En consecuencia, las entidades vigiladas deberán obtener un certificado digital, expedido por una entidad de certificación digital abierta debidamente autorizada por la Superintendencia de Industria y Comercio. Esta firma digital deberá ser adquirida y administrada por las diferentes entidades vigiladas.

Las condiciones, restricciones y el procedimiento técnico para el uso de esta firma digital, estará determinado por las características que brinde la entidad de certificación digital a través de su Declaración de Prácticas de Certificación.

En este sentido, es necesario tener en cuenta consideraciones generales para la utilización de los mensajes de datos y las firmas digitales del sistema electrónico de inspección, vigilancia y control de la Superintendencia Nacional de Salud como las que a continuación se presentan:

### **1. Características que deben satisfacer los certificados y firmas digitales.**

Las comunicaciones electrónicas de cualquier índole enviadas por las entidades vigiladas a la Superintendencia Nacional de Salud, en cumplimiento de las funciones de inspección, vigilancia y control que se encuentren respaldados con una firma digital deberán cumplir con las disposiciones del artículo 28 de la Ley 527 de 1999 con el fin de dar por satisfechos los atributos jurídicos propios de una firma digital, garantizando con ello que dicha firma tendrá la misma fuerza y efectos que el uso de una firma manuscrita. De igual manera, los certificados digitales que respalden dichas firmas deberán cumplir con las disposiciones del artículo 15 del decreto 1747 de 2000, y por lo tanto deben ser emitidos por una entidad de certificación abierta autorizada por la Superintendencia de Industria y Comercio.

### **2. Consideraciones para el intercambio de mensajes de datos firmados digitalmente.**

A continuación se definen las consideraciones que deben ser tenidas en cuenta para el intercambio de mensajes de datos respaldados con firmas digitales:

2.1. Para el envío de comunicaciones emitidas por las entidades vigiladas, así como para la recepción de las comunicaciones dirigidas a éstos se debe hacer uso de los sistemas de comunicación definidos por la Superintendencia Nacional de Salud para tal fin.

2.2. Las comunicaciones en forma de mensajes de datos emitidas por la entidad vigilada que requieran de una firma manuscrita en su equivalente en papel, deberán encontrarse firmadas digitalmente.



2.3. Las comunicaciones en forma de mensajes de datos respaldadas con certificados digitales generadas por la entidad vigilada deberán encontrarse dentro de los usos aceptados en la Declaración de Prácticas de Certificación de la entidad de certificación que emite los certificados.

### **3. Consideraciones para la verificación y validación de mensajes de datos firmados digitalmente por parte de las entidades vigiladas.**

La Superintendencia Nacional de Salud será parte confiante en la recepción de las comunicaciones electrónicas firmadas digitalmente emitidas por sus entidades vigiladas dentro de las funciones propias de inspección, vigilancia y control. En su rol como parte confiante la Superintendencia Nacional de Salud verifica que la firma digital asociada al mensaje de datos o comunicación electrónica satisface:

3.1. Que el certificado digital que respalda la firma digital del acto de comunicación fue emitido por una entidad de certificación abierta autorizada para ello por la Superintendencia de Industria y Comercio.

3.2. Que la firma digital puede ser verificada con la clave pública que se encuentra en el certificado digital en relación con la firma, emitido por la entidad de certificación autorizada.

3.3. Que la firma digital fue emitida dentro del tiempo de validez del certificado.

3.4. Que el certificado digital que respalda la firma digital no haya sido revocado, para este efecto, se debe validar que el certificado digital no se encuentre en la base de datos de certificados digitales revocados publicada por la Entidad de Certificación.

3.5. Que el mensaje de datos goza de integridad.

3.6. Que el mensaje de datos firmado se encuentra dentro de los usos aceptados en la Declaración de Prácticas de Certificación.

De igual forma, la entidad vigilada deberá cumplir con todas las obligaciones que adquiera como suscriptor o parte confiante dentro del Sistema de Certificación Digital de acuerdo con las disposiciones de la Declaración de Prácticas de Certificación de la entidad de certificación.

### **4. Recomendaciones de seguridad para la administración del certificado digital.**

En el presente numeral se establecen las medidas de seguridad necesarias para la



administración del certificado digital, por parte de los vigilados:

- 4.1. El Certificado digital es de carácter personal e intransferible.
- 4.2. No permitir que otras personas conozcan el número de identificación personal clave de protección de acceso al certificado digital.
- 4.3. Si el certificado digital se encuentra almacenado en un dispositivo seguro, este debe estar siempre en poder de su titular o almacenado de manera segura.
- 4.4. No se debe emplear el dispositivo de almacenamiento del certificado digital para almacenar datos, o para propósitos distintos a firmar digital mente mensajes de datos.
- 4.5. Si se extravía o se pierde el control del dispositivo de almacenamiento del certificado digital o de su clave de protección de acceso debe comunicarse inmediatamente con la entidad de certificación que lo emitió, y se deberá solicitar su revocación.
- 4.6 No se debe olvidar la clave de protección de acceso al certificado digital, su olvido implica la revocación del certificado digital y la emisión de un nuevo certificado digital.
- 4.7. Se deben tener en cuenta las políticas de seguridad asociadas con la clave de protección de acceso al certificado digital. Por ejemplo el número máxima de ingresos consecutivos erróneos permitidos dentro del sistema de certificación digital.

## **5. Obligaciones y responsabilidades Generales del suscriptor del certificado digital.**

La entidad vigilada suscriptora del certificado digital tiene las siguientes obligaciones frente a la entidad de certificación y terceras personas en la utilización de su certificado digital:

- 5.1. Utilizar la clave privada y el certificado digital emitido tan solo para los fines establecidos y de acuerdo con los condicionamientos establecidos en la Declaración de Prácticas de Certificación de la entidad de certificación y en el certificado digital entregado. Será responsabilidad del suscriptor el uso indebido que este o terceros hagan del mismo.
- 5.2. Responder por la custodia de la clave privada y de su soporte físico (si aplica) evitando su pérdida, revelación, modificación o uso no autorizado. Especialmente,



el suscriptor deberá abstenerse, sin importar la circunstancia, de anotar en el soporte físico del certificado digital el código de activación o las claves privadas, ni tampoco en cualquier otro documento que el suscriptor conserve o transporte consigo o con el soporte físico.

5.3. Solicitar la revocación del certificado digital que le ha sido entregado cuando se cumpla alguno de los supuestos previstos para la revocación de los certificados digitales, de conformidad con lo dispuesto en la Declaración de Practicas de Certificación de la entidad de certificación.

5.4. Abstenerse en toda circunstancia de revelar la clave privada o el código de activación del certificado digital, así como abstenerse de delegar su uso a terceras personas.

5.5. Asegurarse de que toda la información contenida en el certificado digital es cierta y notificar inmediatamente a la entidad de certificación en caso de que se haya incluido cualquier información incorrecta o inexacta o en caso de que por alguna circunstancia posterior la información del certificado digital no corresponda con la realidad. Así mismo, deberá comunicar de manera inmediata el cambio o variación que haya sufrido cualquiera de los datos que apporto para la emisión del certificado digital, aunque estos no estuvieran incluidos en el propio certificado digital.

5.6. Informar inmediatamente a la entidad de certificación acerca de cualquier situación que pueda afectar la confiabilidad del certificado digital, e iniciar el procedimiento de revocación del certificado digital cuando sea necesario. Especialmente, deberá notificar de inmediato la pérdida, robo o falsificación del soporte físico y cualquier intento de realizar estos actos sobre el mismo, así como el conocimiento por otras personas del código de activación o de las claves privadas, solicitando la revocación del certificado digital de conformidad con el procedimiento que se establece en la Declaración de Practicas de Certificación de la entidad de certificación.

5.7. Abstenerse de monitorear, alterar, realizar ingeniería reversa o interferir en cualquier otra forma la prestación de servicios de certificación digital.

5.8. El suscriptor es el único responsable por las obligaciones que emanen de las operaciones o negocios jurídicos que se realicen con los certificados digitales, exonerando a la entidad de certificación de toda responsabilidad por este concepto.

5.9. Cualquier otra que se derive de la ley, del contenido de la Declaración de Practicas de Certificación de la entidad de certificación.



5.10. Manejo del PIN: Es importante destacar que el PIN de protección del certificado digital es único de uso personal e intransferible, el conocimiento del mismo será solo del suscriptor o usuario final, la Entidad de Certificación Digital no almacena ni asigna los PIN, por lo tanto su olvido implica revocación del Certificado Digital y obliga a la emisión de un nuevo certificado digital.

5.11. La entidad de certificación no tiene deber alguno de investigación o revisión de la ocurrencia de cualquiera de las causales de revocación establecidas en la Declaración de Prácticas de Certificación. La entidad de certificación iniciara el procedimiento de revocación de certificados digitales tan solo una vez tenga noticia de la ocurrencia de cualquiera de ellas. El suscriptor y la parte confiante - en caso de que sea procedente - tienen la obligación de iniciar el procedimiento de revocación del certificado digital tan pronto como tengan conocimiento de la existencia de alguno de estos supuestos.

## **6. Consideraciones para la conservación de mensajes de datos firmados digitalmente y/o cifrados y los certificados digitales.**

La Superintendencia Nacional de Salud, realiza las siguientes recomendaciones para las entidades vigiladas con respecto a la conservación de los mensajes de datos o documentos firmados digitalmente:

6.1. Las comunicaciones electrónicas que se encuentren respaldados por una firma digital avalada por una entidad de certificación autorizada conforme a la ley y que en los términos de esta deban ser conservados, se deberán guardar en condiciones que permitan que la información sea accesible para su posterior consulta y que garanticen que permanezca completa e inalterada.

6.2. La entidad vigilada deberá hacer uso de los mecanismos idóneos para llevar a cabo la conservación de los documentos firmados digitalmente y presentados a la Superintendencia Nacional de Salud, ya que la Superintendencia podrá volver a requerir la información.

6.3. La entidad vigilada será responsable de la conservación de los certificados digitales, su medio de almacenamiento y la clave de acceso al mismo, siempre que estos hayan sido utilizados para el cifrado de mensajes de correo electrónico y/o documentos presentados en forma de mensajes de datos, lo anterior con el fin de garantizar la accesibilidad de los mensajes de datos cifrados para su posterior consulta.

## **7. Consideraciones sobre los responsables en el suministro de la información y el cumplimiento de las instrucciones impartidas por la Superintendencia**



**Nacional de Salud.**

El envío de la información que deben presentar a esta Superintendencia los vigilados a quienes se dirige la Circular Única, es responsabilidad de los representantes legales de las Entidades. (Modificado Circular Externa No. 049 de 2008)

De igual manera, los contadores y revisores fiscales serán responsables en el evento que se suministren datos contrarios a la realidad y/u ordenen, toleren, hagan o encubran falsedad en la información remitida a esta Superintendencia en los términos que señalan los artículos 10 de la Ley 43 de 1990, 207 y siguientes del Código de Comercio y 43 de la Ley 222 de 1995.