POLÍTICA DE CERTIFICACIÓN – CERTIFICADOS DIGITALES

*El Futuro Digital es **Ahora***

Contenido

1. Certificado de persona jurídica - OID: 1.3.6.1.4.1.17326.20.10.5.2	
Certificado de persona jurídica en nube	1.3.6.1.4.1.17326.20.10.5.2 / 0.4.0.2042.1.2 / 1.3.6.1.4.1.17326.99.18.1
Certificado de persona jurídica en tarjeta	1.3.6.1.4.1.17326.20.10.5.2 / 0.4.0.2042.1.2
1.1 Objeto del certificado	
Se trata de un certificado digital emitido a favor de una Entidad jurídica que podrá ser utilizado cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario. El solicitante del certificado deberá tener capacidad para representar a la entidad titular del certificado.	

1.2 Requisitos, procesos y documentos necesarios para la emisión del certificado

1.2.1 Identificación del Solicitante

NIT, Cédula de Ciudadanía, tarjeta de identidad, pasaporte o cualquier otro documento admitido en derecho, siempre que contenga al menos la siguiente información:

- Nombre y apellidos de la persona
- Lugar y fecha de nacimiento
- Número de identidad reconocido legalmente
- Otros atributos de la persona que deban constar en el certificado

1.2.2 Identificación de la entidad

Con carácter previo a la emisión y entrega de un certificado de organización es necesario autenticar los datos relativos a la constitución y la personalidad jurídica de la entidad. Se exige la identificación de la entidad, por lo que la AR requerirá la documentación pertinente en función del tipo de entidad. Esta información varía dependiendo del tipo de entidad y está indicada en los manuales operativos de la AR y en la Web de la SubCA. En general serán datos relativos a la constitución y la personalidad jurídica de la entidad, y a la extensión y vigencia de las facultades o poderes de representación del solicitante, mediante los documentos públicos que los acrediten de forma fehaciente y la consulta al pertinente registro público, cuando se trate de datos que deben figurar en ella. Se comprobará:

- Nombre legal completo de la organización
- Estado legal de la organización
- Número de registro tributario
- Datos de identificación registral
- Certificado de existencia y representación legal expedida por la entidad competente (no superior a 30 días) o documento equivalente para las entidades públicas.

Nota. Para el caso de las entidades públicas, acta de posesión de nombramiento o documento que acredite la condición como funcionario público que especifique el cargo que desempeña o acta de adjudicación o contrato que acredite la legitimidad del solicitante del certificado.

1.2.3 Decreto 2460 de 2013 Código de Comercio (Artículo 27)

En los Certificados de persona jurídica, en los que el Firmante/ Suscriptor y el Solicitante son distintos, deberá demostrar documentalmente que el Solicitante tiene poderes suficientes para realizar dicha solicitud de certificado por cuenta del Firmante/ Suscriptor, mediante la presentación de un certificado del registro público correspondiente no superior a 10 días o mediante consulta en línea realizada por la propia AR a los datos del registro público correspondiente.

En caso de la que organización este constituida en el extranjero sin sucursal en Colombia se requiere:

a) Documento emitido por la autoridad competente en el país de su domicilio, expedido por lo menos dentro de los treinta (30) días anteriores a la fecha de solicitud del certificado, en el que debe constar. (i) La existencia de la sociedad, su objeto social y nombre del representante legal; (ii) La capacidad jurídica, facultades y limitaciones del representante legal y (iii) La fecha de constitución y de duración de la sociedad.
b) En el evento en que conforme a la jurisdicción de la persona jurídica no hubiese un documento que contenga la totalidad de la información requerida, presentarán los documentos que sean necesarios para acreditar lo solicitado expedidos por las respectivas autoridades competentes del país de origen. Si en la jurisdicción respectiva no existiese ninguna autoridad o entidad que certifique la totalidad de la información aquí solicitada, la persona jurídica extranjera deberá presentar una declaración juramentada de una persona con capacidad jurídica para vincular y representar a la sociedad en la que conste que (i) no existe autoridad u organismo que certifique lo solicitado; y (ii) la capacidad jurídica para vincular y representar a la sociedad de la persona que efectúa la declaración, así como de las demás personas que puedan representar y vincular a la sociedad, si las hay. A efectos de esta declaración se podrá diseñar un modelo prediseñado con un texto sugerido.
c) Los documentos presentados deberán ser legalizados y/o apostillados, de conformidad con la normativa aplicable.
d) En todo caso, para la emisión del certificado se podrán solicitar los demás soportes y documentos necesarios de acuerdo al país de origen, para tener certeza de la información necesaria para la emisión del certificado

2. Certificado de persona natural - OID: 1.3.6.1.4.1.17326.20.10.1.2	
Certificado de persona natural en nube	1.3.6.1.4.1.17326.20.10.1.2 / 0.4.0.2042.1.2 / 1.3.6.1.4.1.17326.99.18.1
Certificado de persona natural en tarjeta	1.3.6.1.4.1.17326.20.10.1.2 / 0.4.0.2042.1.2
2.1 Objeto del certificado	
El certificado digital de persona natural, sirve exclusivamente para que una persona natural se identifique como tal y su uso se restringe para realizar todo tipo de trámites como Persona Natural como son firmar mensajes de datos y/o documentos.	

La Entidad realizará el proceso de emisión del certificado se guiará con base en lo establecido en el presente documento y la DPC. Las decisiones que se deban tomar en el marco de este proceso se sustentarán en razones eminentemente objetivas y, por ende, no se sustentarán en criterios que puedan ser discriminatorios

2.2 Requisitos, procesos y documentos necesarios para la emisión del certificado

2.2.1 Identificación del Solicitante

Cédula de Ciudadanía, tarjeta de identidad, pasaporte o cualquier otro documento admitido en derecho, siempre que contenga al menos la siguiente información:

- Nombre y apellidos de la persona
- Lugar y fecha de nacimiento
- Número de identidad reconocido legalmente
- Otros atributos de la persona que deban constar en el certificado

3. Certificado de pertenencia a empresa - OID: 1.3.6.1.4.1.17326.20.10.4.2	
Certificado de pertenencia a empresa en nube	1.3.6.1.4.1.17326.20.10.4.2 / 0.4.0.2042.1.2 / 1.3.6.1.4.1.17326.99.18.1
Certificado de pertenencia a empresa tarjeta	1.3.6.1.4.1.17326.20.10.4.2 / 0.4.0.2042.1.2
3.1 Objeto del certificado	
El certificado digital de pertenencia a entidad garantiza la identidad de la persona física titular del certificado, así como su vinculación a una determinada Entidad en virtud del cargo que ocupa en la misma.	

3.2 Requisitos, procesos y documentos necesarios para la emisión del certificado

3.2.1 Identificación del Solicitante

Cédula de Ciudadanía, tarjeta de identidad, pasaporte o cualquier otro documento admitido en derecho, siempre que contenga al menos la siguiente información:

- Nombre y apellidos de la persona
- Lugar y fecha de nacimiento
- Número de identidad reconocido legalmente
- Otros atributos de la persona que deban constar en el certificado
- Carta Laboral o documento equivalente que acredite el cargo que desempeña (No superior a 30 días)
- RUT de la entidad o personal jurídica
- Certificado de existencia y representación legal expedida por la entidad competente (No superior a 30 días)

3.2.2 Identificación de la entidad

Con carácter previo a la emisión y entrega de un certificado de organización es necesario autenticar los datos relativos a la constitución y la personalidad jurídica de la entidad. Se exige la identificación de la entidad, por lo que la AR requerirá la documentación pertinente en función del tipo de entidad. Esta información varía dependiendo del tipo de entidad y está indicada en los manuales operativos de la AR y en la Web de la SubCA. En general serán datos relativos a la constitución y la personalidad jurídica de la entidad, y a la extensión y vigencia de las facultades o poderes de representación del solicitante, mediante los documentos públicos que los acrediten de forma fehaciente y la consulta al pertinente registro público, cuando se trate de datos que deben figurar en ella.

4. Certificado de representante de empresa - OID: 1.3.6.1.4.1.17326.20.10.3.2	
Certificado de representante de empresa en nube	1.3.6.1.4.1.17326.20.10.3.2 / 0.4.0.2042.1.2 / 1.3.6.1.4.1.17326.99.18.1
Certificado de representante de empresa en tarjeta	1.3.6.1.4.1.17326.20.10.3.2 / 0.4.0.2042.1.2
4.1 Objeto del certificado	
El certificado digital de representante es emitido a favor de una persona física representante de una determinada Entidad. El titular del certificado se identifica no únicamente como persona física perteneciente a una empresa, sino que añade su cualificación como representante legal o apoderado general de la misma. La solicitud de un certificado de representante está limitada únicamente a los representantes legales (administradores) o a quienes ostentan un poder notarial general para actuar en nombre y representación de la Entidad.	

4.2 Requisitos, procesos y documentos necesarios para la emisión del certificado

4.2.1 Identificación del solicitante

NIT, Cédula de Ciudadanía, tarjeta de identidad, pasaporte o cualquier otro documento admitido en derecho, siempre que contenga al menos la siguiente información:

- Nombre y apellidos de la persona
- Lugar y fecha de nacimiento
- Número de identidad reconocido legalmente
- Otros atributos de la persona que deban constar en el certificado

4.2.2 Identificación de la entidad

Con carácter previo a la emisión y entrega de un certificado de organización es necesario autenticar los datos relativos a la constitución y la personalidad jurídica de la entidad. Se exige la identificación de la entidad, por lo que la AR requerirá la documentación pertinente en función del tipo de entidad. Esta información varía dependiendo del tipo de entidad y está indicada en los manuales operativos

de la AR y en la Web de la SubCA. En general serán datos relativos a la constitución y la personalidad jurídica de la entidad, y a la extensión y vigencia de las facultades o poderes de representación del solicitante, mediante los documentos públicos que los acrediten de forma fehaciente y la consulta al pertinente registro público, cuando se trate de datos que deben figurar en ella. Se solicitará documentos (además del documento de identificación):

- RUT de la entidad o persona jurídica
- Certificado de existencia y representación legal expedida por la entidad competente (No superior a 30 días)

En caso de la que organización este constituida en el extranjero sin sucursal en Colombia se requiere:

a) Documento emitido por la autoridad competente en el país de su domicilio, expedido por lo menos dentro de los treinta (30) días anteriores a la fecha de solicitud del certificado, en el que debe constar. (i) La existencia de la sociedad, su objeto social y nombre del representante legal; (ii) La capacidad jurídica, facultades y limitaciones del representante legal y (iii) La fecha de constitución y de duración de la sociedad.
b) En el evento en que conforme a la jurisdicción de la persona jurídica no hubiese un documento que contenga la totalidad de la información requerida, presentarán los documentos que sean necesarios para acreditar lo solicitado expedidos por las respectivas autoridades competentes del país de origen. Si en la jurisdicción respectiva no existiese ninguna autoridad o entidad que certifique la totalidad de la información aquí solicitada, la persona jurídica extranjera deberá presentar una declaración juramentada de una persona con capacidad jurídica para vincular y representar a la sociedad en la que conste que (i) no existe autoridad u organismo que certifique lo solicitado; y (ii) la capacidad jurídica para vincular y representar a la sociedad de la persona que efectúa la declaración, así como de las demás personas que puedan representar y vincular a la sociedad, si las hay. A efectos de esta declaración se podrá diseñar un modelo prediseñado con un texto sugerido.
c) Los documentos presentados deberán ser legalizados y/o apostillados, de conformidad con la normativa aplicable.
d) En todo caso, para la emisión del certificado se podrán solicitar los demás soportes y documentos necesarios de acuerdo al país de origen, para tener certeza de la información necesaria para la emisión del certificado

Además, se exige la documentación sobre la capacidad de representación del Firmante/Suscriptor respecto de la otra persona, por medio de la entrega de las escrituras notariales que demuestran sus poderes o facultades de representación. Se presentará un certificado expedido por el registro público correspondiente con menos de 10 días de antigüedad. La AR puede disponer también de medios telemáticos para la consulta en línea del estado y nivel de representación del solicitante.

5. Certificado de apoderado - OID: 1.3.6.1.4.1.17326.20.10.6.2	
Certificado de apoderado en nube	1.3.6.1.4.1.17326.20.10.6.2 / 0.4.0.2042.1.2 / 1.3.6.1.4.1.17326.99.18.1
Certificado de apoderado en tarjeta	1.3.6.1.4.1.17326.20.10.6.2 / 0.4.0.2042.1.2
5.1 Objeto del certificado	
El certificado de apoderado determina la relación de representación específica o de apoderamiento especial (con facultades limitadas) entre una persona física (titular del certificado/firmante/suscriptor) y una Entidad (descrita también en el campo Organización del certificado).	

5.2 Requisitos, procesos y documentos necesarios para la emisión del certificado

5.2.1 Identificación del Solicitante

NIT, Cédula de Ciudadanía, tarjeta de identidad, pasaporte o cualquier otro documento admitido en derecho, siempre que contenga al menos la siguiente información:

- Nombre y apellidos de la persona
- Lugar y fecha de nacimiento
- Número de identidad reconocido legalmente
- Otros atributos de la persona que deban constar en el certificado

5.2.2 Identificación de la entidad

Con carácter previo a la emisión y entrega de un certificado de organización es necesario autenticar los datos relativos a la constitución y la personalidad jurídica de la entidad, mediante los documentos:

- Poder otorgado ante notario público
- Si es un poder otorgado en el extranjero deberá presentarse apostillado ante ministerio de relaciones exteriores
- En caso de poder general deberá presentar la escritura pública correspondiente

6. Certificado de función pública - OID: 1.3.6.1.4.1.17326.20.10.2.2	
Certificado de función pública en nube	1.3.6.1.4.1.17326.20.10.2.2 / 0.4.0.2042.1.2 / 1.3.6.1.4.1.17326.99.18.1
Certificado de función pública en tarjeta	1.3.6.1.4.1.17326.20.10.2.2 / 0.4.0.2042.1.2
6.1 Objeto del certificado	
Certificado que tiene por objeto identificar a los empleados públicos, así como su vinculación a una concreta Administración Pública en virtud del cargo que ocupa en la misma.	

6.2 Requisitos, procesos y documentos necesarios para la emisión del certificado

6.2.1 Identificación del Solicitante

NIT, Cédula de Ciudadanía, tarjeta de identidad, pasaporte o cualquier otro documento admitido en derecho, siempre que contenga al menos la siguiente información:

- Nombre y apellidos de la persona
- Lugar y fecha de nacimiento
- Número de identidad reconocido legalmente
- RUT de la entidad o persona Jurídica
- Acta de posesión de nombramiento o documento que acredite la condición como funcionario público que especifique el cargo que desempeña

6.2.2 Identificación de la entidad

NIT, Cédula de Ciudadanía, tarjeta de identidad, pasaporte o cualquier otro documento admitido en derecho, siempre que contenga al menos la siguiente información:

- Nombre y apellidos de la persona
- Lugar y fecha de nacimiento
- Número de identidad reconocido legalmente
- Otros atributos de la persona que deban constar en el certificado

No se exige la documentación acreditativa de la existencia de la administración pública. Se exige la documentación de identidad de la persona que actúa como responsable, en nombre de dicha Administración Pública, organismo o entidad de derecho público. El Solicitante / responsable se identificará ante la AR con un documento que acredite de forma fehaciente su identidad y un documento acreditativo de su pertenencia como empleado en la Administración Pública, organismo o entidad de derecho público donde consten además los datos identificativos de ésta.

6. CERTIFICADO DE SERVIDOR SEGURO SSL (OV-EV)

Servicio no acreditado por el Organismo Nacional de Acreditación en Colombia

Emitidos a aplicativos servidores de páginas HTML en Internet mediante protocolo SSL/TLS o HTTPS. Este protocolo es necesario para la identificación y el establecimiento de canales seguros entre el navegador del usuario o tercero que confía y el servidor de páginas HTML del Firmante/Suscriptor.

6.2. Requisitos, procesos y documentos necesarios para la emisión del certificado

6.2.1. Identificación del Solicitante

Con carácter previo a la emisión y entrega de un certificado de organización es necesario autenticar los datos relativos a la constitución y la personalidad jurídica de la entidad.

- Autorización de solicitud
- Cedula del solicitante
- Documento de constitución de la entidad o su equivalente

6.2.2. Comprobación del dominio

Con carácter previo a la emisión y entrega del certificado debe realizarse la comprobación de los dominios para los que se va a emitir el certificado, corroborando que estos dominios están registrados a nombre de la entidad que los solicita

- Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f/ y g) del artículo 26 de la Ley 527 de 1999
- Ofrecer o facilitar los servicios de generación de los datos de creación de las firmas digitales certificadas
- Ofrecer o facilitar los servicios de generación de datos de creación de las firmas electrónicas

7. MARCO LEGAL

"Actividades de Certificación" según el Artículo 161 del Decreto Ley 0019 de 2012 y antes en el artículo 30 de la Ley 527 de 1999:

- Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas
- Ofrecer o facilitar los servicios de generación de los datos de creación de las firmas digitales certificadas
- Ofrecer o facilitar los servicios de generación de datos de creación de las firmas electrónicas.

El perfil del certificado con los estándares, las normas técnicas y reglamentarias, las políticas específicas que establecen los requisitos y fuente reguladora se encuentra disponible en la página web https://camerfirma.com.co/

8. OBLIGACIONES DE LAS PARTES

8.1 Obligaciones del Firmante/Suscriptor

El Firmante/Suscriptor estará obligado a cumplir con lo dispuesto por la normativa vigente y a:

- Usar el certificado según lo establecido en la presente DPC y en las Políticas de Certificación aplicables, manteniendo su control y seguridad.
- Respetar lo dispuesto en los documentos firmados con la SubCA y la AR.

- Informar a la mayor brevedad posible de la existencia de alguna causa de suspensión o revocación.
- Notificar cualquier inexactitud o cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- No utilizar la clave privada ni el certificado una vez la SubCA solicita o informa de la suspensión o revocación del mismo, o una vez ha expirado el plazo de validez del certificado.
- Hacer uso del certificado digital con el carácter de personal e intransferible y, por tanto, asumir la responsabilidad por cualquier actuación que se lleve a cabo en contravención de esta obligación, así como cumplir las obligaciones que sean específicas de la normativa aplicable a las dichas certificaciones digitales.
- Autorizar a la SubCA para proceder al tratamiento de los datos personales contenidos en los certificados, en conexión con las finalidades de la relación electrónica y, en todo caso, para cumplir las obligaciones legales de verificación de certificados.
- Responsabilizarse de que toda la información incluida, por cualquier medio, la solicitud del certificado y en el mismo certificado sea exacta, completa para la finalidad del certificado y esté actualizada en todo momento.
- No utilizar la clave privada, el certificado electrónico o cualquier otro soporte técnico entregado por el prestador de servicios de certificación correspondiente para realizar ninguna transacción prohibida por la ley aplicable.
- Los suscriptores serán responsables por la falsedad, error u omisión en la información suministrada a la entidad de certificación y por el incumplimiento de sus deberes como suscriptor
- Generar sus claves de suscriptor utilizando un algoritmo reconocido como aceptable para la firma electrónica, en su caso cualificado, o el sello electrónico, en su caso calificado.

Si el suscriptor genera sus propias claves, se obliga a:

- Generar sus claves de suscriptor utilizando un algoritmo reconocido como aceptable para la firma electrónica, en su caso cualificado, o el sello electrónico, en su caso calificado.
- Crear las claves dentro del dispositivo de creación de firma o de sello, utilizando un dispositivo seguro cuando proceda.
- Utilizar longitudes y algoritmos de clave reconocidos como aceptables para la firma electrónica.

8.2 Obligaciones del Solicitante del certificado

El Solicitante de un certificado ya sea de forma directa o a través de un tercero autorizado) se compromete a cumplir con las disposiciones legales y a:

- Utilizar el certificado de acuerdo con la presente DPC y las Políticas de Certificación aplicables.
- Respetar las disposiciones establecidas en los documentos suscritos con la SubCA y la RA
- Reportar cualquier causa de suspensión / revocación tan pronto como sea posible.

- Reporte cualquier cambio en los datos proporcionados para crear el certificado durante su período de validez.
- No utilizar la clave privada ni el certificado una vez la SubCA solicita o informa de la suspensión o revocación del mismo, o una vez ha expirado el plazo de validez del certificado

8.3 Obligaciones del Tercero de confianza/Usuario

Será obligación del Tercero que confía cumplir con lo dispuesto en la normativa vigente y a:

- Verificar la validez de los certificados antes de realizar cualquier operación basada en los mismos. la SubCA dispone de diversos mecanismos para realizar dicha comprobación, como el acceso a listas de revocación o a servicios de consulta en línea como OCSP, todos estos mecanismos están descritos en la página Web de la SubCA indicada en la sección 1.3.

- Conocer y respetar las garantías, limitaciones y responsabilidades aplicables con la aceptación y uso de los certificados de confianza, y aceptar estar sujeto a ellas.

8.4 Obligaciones de la Entidad

La Entidad estará obligada a solicitar a la AR la revocación o suspensión del certificado cuando el Firmante/Suscriptor cese dicha vinculación respecto a la organización.

La Entidad realizará el proceso de emisión del certificado se guiará con base en lo establecido en el presente documento y la DPC. Las decisiones que se deban tomar en el marco de este proceso se sustentarán en razones eminentemente objetivas y, por ende, no se sustentarán en criterios que puedan ser discriminatorios.

9. RESPONSABILIDAD DE LAS PARTES

9.1 Responsabilidad de los suscriptores

Los suscriptores serán responsables por la falsedad, error u omisión en la información suministrada a la SubCA o AR y por el incumplimiento de sus deberes como suscriptor (art. 40, Ley 527 de 1999).

9.2 Exoneración de responsabilidad de AC y AR

Según la legislación vigente, la responsabilidad de la AC y de la AR no se extiende a aquellos supuestos en los que la utilización indebida del certificado tiene su origen en conductas imputables al Firmante y al Tercero de confianza por:

- No haber proporcionado la información correcta, inicial o posteriormente como consecuencia de modificaciones de las circunstancias reflejadas en el certificado electrónico, cuando su inexactitud no haya podido ser detectada por el Prestador de Servicios de Certificación.

- Haber incurrido en negligencia con respecto a la conservación de los datos de creación de firma y a su confidencialidad.
- No haber solicitado la suspensión o revocación del certificado electrónico en caso de duda sobre el mantenimiento de la confidencialidad.
- Haber utilizado la firma después de haber expirado el periodo de validez del certificado electrónico.
- Superar los límites que figuren en el certificado electrónico.
- En conductas imputables al Tercero que confía si éste actúa de forma negligente, es decir cuando no compruebe o tenga en cuenta las restricciones que figuran en el certificado en cuanto a sus posibles usos y límite de número de transacciones; o cuando no tenga en cuenta el estado de vigencia del certificado.
- De los daños ocasionados al firmante o terceros que confía por la inexactitud de los datos que consten en el certificado electrónico, si éstos le han sido acreditados mediante documento público, inscrito en un registro público, si así resulta exigible.

La AC y las AR tampoco serán responsables en ningún caso cuando se encuentran ante cualquiera de estas circunstancias: La AC y las AR tampoco serán responsables en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.
- Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y en las Políticas de Certificación.
- Por el uso indebido o fraudulento de los certificados o CRL's emitidos por la AC.
- Por el uso de la información contenida en el Certificado o en la CRL.
- Fraude en la documentación presentada por el Solicitante.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación o suspensión.
- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Por el incumplimiento de las obligaciones establecidas para el Firmante/Suscriptor o Terceros que confían en la normativa vigente, en las Políticas de Certificación o en esta DPC.
- Por la no recuperación de documentos cifrados con la clave pública del Firmante. y límite de número de transacciones; o cuando no tenga en cuenta el estado de vigencia del certificado.
- Por la no recuperación de documentos cifrados con la clave pública del Firmante

10. DERECHOS DE LOS SUSCRIPTORES

- Usar el certificado de conformidad con las Políticas de Certificación de cada tipo de certificado establecidas en la DPC.
- A que la ECD le preste los servicios en las condiciones previstas en la normativa vigente y en lo previsto en la PC y DPC.
- Su información sea tratada conforme a la política de protección de datos personales.
- Se conserve de forma adecuada la información sobre los certificados que le hayan sido emitidos conforme a la normativa vigente.

- A solicitar la revocación de sus certificados ya sea por su voluntad o por compromiso de su clave privada

11. INDEPENDENCIA, IMPARCIALIDAD Y NO DISCRIMINACIÓN

Camerfirma debe salvaguardar la imparcialidad e independencia de las actividades de certificación; para esta actividad se dispuso de un comité de imparcialidad e independencia que vigila y monitorea los riesgos que comprometan este aspecto, cualquier conflicto de interés que sea detectado por parte del público en general puede ser reportado en http://https://camerfirma.com.co//contacto/ y se direccionará a esta instancia.

Las actividades de Camerfirma se realizarán de forma imparcial y objetiva, atendiendo en todo momento a las disposiciones consagradas en el presente documento, la DPC y la normativa aplicable

12. MODELO Y CONDICIONES CONTRACTUALES

Las condiciones contractuales y de uso del certificado se exponen al momento de confirmar la solicitud del certificado digital mediante los "Términos y condiciones generales del servicio de certificación digital", dichas disposiciones se elaboran con base en la normatividad aplicable a las actividades de certificación digital y los lineamientos propios de las mismas, expuestas en el desarrollo del presente documento y la Declaración de Practicas de Certificación expuesta en la web de Camerfirma. Los términos y condiciones se encuentran publicados en nuestra página web de https://camerfirma.com.co/

13. DISPOSITIVOS CRIPTOGRÁFICOS USADOS

Los dispositivos criptográficos usados por Camerfirma para el almacenamiento de los certificados (Token-HSM), cumplen con el estándar dispuesto en el documento normativo del ONAC bajo las condiciones del FIPS 140.2 Level 3.

13.1 Contenido de los certificados

Como regla general, los certificados emitidos tendrán la siguiente información, de conformidad con lo señalado en el artículo 35 de la Ley 527 de 1999:

1. Nombre, dirección y domicilio del suscriptor.
2. Una Identificación única del suscriptor nombrado en el certificado
3. El nombre y el lugar donde realiza actividades la entidad de certificación
4. Llave pública del certificado.
5. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
6. El número de serie (único) del certificado
7. Fecha de emisión y expiración del certificado.
8. Código de acreditación asignado por ONAC, incluido como una extensión del certificado

14. PUBLICACIÓN Y COPIA

La presente PC se encontrará publicada en el sitio web de la SubCA. Las versiones anteriores podrán ser solicitadas mediante los canales dispuestos en la misma página web.