



**Agència Catalana  
de Certificació**

Passatge de la Concepció, 11  
08008 Barcelona  
Tel. +34 932 722 600  
Fax +34 932 722 539  
info@catcert.net  
www.catcert.net

## **CONDICIONES GENERALES DEL SERVICIO DE CERTIFICACIÓN DIGITAL DE CLASE 1.**

### **PRIMERA. Objeto y documentación de los servicios**

Estas condiciones generales regulan los servicios de certificación de la Agència Catalana de Certificació (en lo sucesivo, CATCert) a la institución solicitante de servicios, que se convierte en subscriptora de los certificados, identificada en el convenio de prestación del servicio.

Las condiciones generales regulan las cláusulas necesariamente aplicables a todas las instituciones subscriptoras de los servicios de certificación, en atención al carácter común y compartido de la Entidad de Certificación, mientras que el convenio de la prestación de servicios – condiciones particulares, regula las particularidades y personalizaciones de cada institución.

Los servicios de certificación de CATCert se regulan técnicamente y operativamente por la Declaración de prácticas de certificación de la Entidad de Certificación de CATCert (en lo sucesivo, DPC) y por sus actualizaciones posteriores, así como por documentación complementaria suministrada a la institución.

La DPC y la documentación de operaciones de CATCert, que se modifican periódicamente en Registro de certificación y son consultables en la página <http://www.catcert.net/registre>, se incorporan a este convenio por referencia. En caso de discrepancia, el significado de los términos contenidos en este convenio prevalece respecto del que se establece en la DPC.

## **SEGUNDA.** Características de los certificados

### 2.1. Certificado personal de identificación y firma reconocida

Los certificados personales de identificación y firma reconocida (en lo sucesivo, CPISR-1) son certificados reconocidos de acuerdo con lo que se establece en el artículo 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Los CPISR-1 son certificados reconocidos que funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y que dan cumplimiento a aquello dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

De ahí que, los CPISR-1 garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permiten la generación de la “firma electrónica reconocida”; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada empleando un dispositivo seguro, por lo cual, de acuerdo con el que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requerimiento adicional.

Por su parte, los certificados CPISR-1 con cargo incluyen una manifestación relativa a la categoría de personal y cargo del poseedor de claves, que han sido comprobados antes de emitir el certificado, y son correctos. Aún así, esta indicación no es, por sí sola, suficiente por determinar las facultades que tiene el poseedor de claves para firmar en nombre del suscriptor; por lo tanto, el usuario del certificado tendrá que comprobar las facultades y poderes de firma del poseedor mediante otros medios, diferentes al certificado.

Por otra parte, los CPISR-1 se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, sino sólo la identificación del poseedor de claves, en nombre del suscriptor, como las aplicaciones que se indican a continuación:

- a) Autenticación en sistemas de control de acceso

- b) Firma de correo electrónico seguro
- c) Otras aplicaciones de firma digital

La firma electrónica generada en el uso de estas aplicaciones tendrá los efectos que determine la normativa reguladora de la aplicación, que podrá declarar la equivalencia con la firma escrita o sólo el efecto de identificación, puesto que, cuando menos, esta firma habrá sido producida con el dispositivo seguro.

Los CPISR-1 son certificados para personal del subscriptor, dentro de su ámbito corporativo, y no emitidos para el público. Este personal tiene la consideración de poseedor de claves y de la tarjeta y el software complementario correspondientes.

Los CPISR se identifican con el identificador de objeto (OID):  
CPISR de clase 1: 1.3.6.1.4.1.15096.1.3.1.81.

## 2.2. Certificado personal de cifrado

Los certificados personales de cifrado (en lo sucesivo, CPX-1) no son certificados reconocidos, y se pueden utilizar para cifrar documentos propios o para recibir documentos confidenciales, en cualquier formato, protegidos mediante el cifrado del documento por parte del emisor del mensaje utilizando:

- a) La clave pública del poseedor de claves indicada en el CPX.
- b) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública del poseedor de claves indicada en el CPX.

El poseedor de la clave ha de utilizar su clave privada para descifrar el mensaje.

Los CPX garantizan la identidad del subscriptor, pero no permiten la generación de firmas electrónicas de mensajes.

La clave privada del CPX ha de estar archivada para que pueda ser recuperada posteriormente, en las condiciones establecidas en este convenio.

Los CPX se identifican con el identificador de objeto (OID):  
CPX de clase 1: 1.3.6.1.4.1.15096.1.3.1.41.

### 2.3. Certificado de Entidad de Firma Reconocida de Clase 1.

Los certificados de Entidad de Firma Reconocida de clase 1 (en lo sucesivo, CESR-1) son certificados reconocidos de acuerdo con lo que se establece en el artículo 7 y 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Los CESR-1 son certificados reconocidos que funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y que dan cumplimiento a aquello dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

De ahí que, los CESR-1 garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permiten la generación de la “firma electrónica reconocida”; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada empleando un dispositivo seguro, por lo cual, de acuerdo con el que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requerimiento adicional.

Por otra parte, los CESR-1 se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, sino sólo la identificación del poseedor de claves, en nombre de la Institución, como las aplicaciones que se indican a continuación:

- a. Autenticación en sistemas de control de acceso
- b. Firma de correo electrónico seguro
- c. Otras aplicaciones de firma digital

La firma electrónica generada usando estas aplicaciones tendrá los efectos que determine la normativa reguladora de aplicación, que podrá declarar la equivalencia con la firma escrita o sólo el efecto de identificación, puesto que, cuando menos, esta firma habrá sido producida con el dispositivo seguro.

Los CESR-1 son certificados para la Institución, y no emitidos para el público. El personal de la Institución que recibe el certificado tiene la consideración de

poseedor y responsable de custodia de las claves, así como de la tarjeta y el software complementario correspondientes.

Los CESR-1 se identifican con el identificador del objeto (OID):

CESR de clase 1: 1.3.6.1.4.1.15096.1.3.1.121.

#### 2.4. Certificado de Entidad de Cifrado de Clase 1.

Los certificados de entidad de cifrado de clase 1 (en lo sucesivo, CEX-1) son certificados reconocidos de acuerdo con lo que se establece en el artículo 7 y 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Los CEX-1 son certificados reconocidos que funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y que dan cumplimiento a aquello dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

De ahí que, los CEX-1 garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permiten cifrar documentos y recibir mensajes de datos confidenciales, en cualquier formato, protegidos mediante el cifrado del texto del mensaje por parte del emisor del mensaje utilizando:

- a. La clave pública del poseedor de claves indicada al CEX-1
- b. Una clave de cifrado de sesión, simétrica, cifrada con la clave pública del poseedor de claves indicada al CEX-1.

El poseedor de la clave ha de utilizar su clave privada para descifrar el mensaje.

Los CEX-1 garantizan la identidad del suscriptor pero no permiten la generación de firmas electrónicas de mensajes.

La clave privada del CEX-1 ha de estar archivada para que pueda ser recuperada posteriormente, en las condiciones establecidas en este anexo.

Los CEX-1 se identifican con el identificador del objeto (OID):  
CEX de clase 1: 1.3.6.1.4.1.15096.1.3.1.131.

## 2.5. Tarjeta de poseedor de claves

Los certificados CPISR-1 y CPX-1, así como los certificados CESR-1 y CEX-1 se emiten conjuntamente, dentro de la tarjeta del poseedor de claves, que tiene la consideración de dispositivo seguro de creación de firma.

## 2.6. Certificado de dispositivo de firma de software

Los certificados de firma de software (CDP-1) se emiten a personas jurídicas responsables de la edición, publicación o distribución digitales de software informático para la firma del software, que permite instalarlo o ejecutarlo a distancia.

Los CDP se identifican con el identificador de objeto (OID):  
CDP de clase 1: 1.3.6.1.4.1.15096.1.3.1.71.

## 2.7. Certificado de dispositivo servidor seguro

Los certificados de dispositivo servidor seguro (CDS-1) se emiten a personas jurídicas, responsables de la operación de servidores seguros con el sistema SSL de Netscape o TLS, de acuerdo con la RFC 2246 de la IETF, con los usos siguientes:

- Autenticación de servidor
- Cifrado de las comunicaciones entre cliente y servidor

Los CDS se identifican con el identificador de objeto (OID):  
CDS de clase 1: 1.3.6.1.4.1.15096.1.3.1.51.

## 2.8. Certificado de dispositivo de aplicación digitalmente asegurada

Los certificados de dispositivo de aplicación digitalmente asegurada (en lo sucesivo, CDA-1) se emiten a personas jurídicas responsables de la operación de aplicaciones informáticas que se identifican digitalmente, firman electrónicamente webservices u otros protocolos y que reciben documentos y mensajes cifrados.

Los CDA se identifican con el identificador de objeto (OID):  
CDA de clase 1: 1.3.6.1.4.1.15096.1.3.1.91.

## 2.9. Certificado de objeto sobre digital administrativo

Los certificados de objeto sobre digital administrativo se emiten a los órganos de contratación del suscriptor, para el cifrado de los documentos de las licitaciones telemáticas.

Los COS se identifican con el identificador de objeto (OID):  
COS de clase 1: 1.3.6.1.4.1.15096.1.3.1.101.

## 2.10. Duración de los certificados

Todos los certificados emitidos de acuerdo con este convenio tendrán un periodo máximo de validez de cuatro años desde el día en que sean emitidos.

La fecha de expiración de los certificados figura indicada dentro los mismos certificados.

## **TERCERA. Obligaciones del suscriptor**

### 3.1. Solicitud de servicio y generación de las claves

El suscriptor solicitará y autorizará a CATCert, o a la entidad de registro que seleccione, para que:

- a) Genere las claves del suscriptor, privada y pública, para la identificación y la firma electrónica dentro de un dispositivo seguro de creación de firma electrónica (la tarjeta que recibe el poseedor de claves), y realice la emisión del certificado CPISR, CPX, CESR, CEX, CDP, CDS o CDA correspondiente.
- b) Genere las claves privada y pública, para la funcionalidad de cifrado. Esta clave será insertada en el dispositivo de descifrado (la tarjeta que recibe el poseedor de claves) y entregada, una vez se haya generado el certificado CPX o CEX.
- c) Almacene una copia de la clave privada de descifrado, con las medidas de seguridad necesarias, para que personas debidamente autorizadas puedan acceder, para poder recuperar la clave privada

en caso de que el poseedor de claves la pierda o por la simple voluntad del suscriptor, sin que sea necesario alegar ninguna causa legítima.

### 3.2. Personal responsable de la ejecución de los procedimientos

El suscriptor se obliga a nombrar a las siguientes personas:

- a) Una o más personas a su servicio, denominadas “responsables del servicio”, que actuarán como interlocutores con CATCert en todo aquello referido a los servicios de certificación.
- b) Dos o más personas a su servicio, denominadas “solicitantes”, para realizar las solicitudes de emisión, suspensión, alzamiento de la suspensión, revocación y renovación de los certificados de acuerdo con los procedimientos suministrados por CATCert.
- c) Dos o más personas a su servicio, denominadas “certificadores”, para aportar la justificación documental necesaria para el registro de usuarios por CATCert y la posterior emisión de certificados.

### 3.3. Veracidad de la información

El suscriptor se responsabilizará de que toda la información incluida, por cualquier medio, en la solicitud del certificado y en el mismo certificado sea exacta, completa para la finalidad del certificado y esté actualizada en todo momento.

El suscriptor puede delegar en CATCert o en la entidad de registro colaboradora que seleccione, delegación sometida a aceptación posterior, la ejecución y la responsabilidad asociada de las funciones de entidad de registro de los certificados.

El suscriptor ha de informar inmediatamente a CATCert de cualquier inexactitud en el certificado detectada una vez se haya emitido, así como de los cambios que se produzcan en la información aportada por el suscriptor para la emisión del certificado.

En el supuesto de que un poseedor de claves a quien se haya emitido un certificado cese en su vinculación con el suscriptor, éste tiene que solicitar inmediatamente la revocación del certificado.

### 3.4. Entrega y aceptación del servicio

Con la firma de la hoja de entrega, el suscriptor y, si cabe, el poseedor de claves reconocen que se les han entregado la tarjeta, el certificado, la clave privada y cualquier otro soporte técnico entregado por CATCert, así como, en su caso, el código de identificación personal, y que estos elementos funcionan correctamente.

El suscriptor y, si cabe, el poseedor de claves aceptan, con la firma de la hoja de entrega, el certificado. Asimismo, el suscriptor queda vinculado por los términos de la política de certificado aplicable, según se especifica en la Declaración de prácticas de certificación de CATCert.

El poseedor acepta el certificado mediante el procedimiento telemático de aceptación de certificados descrito a la DPC de CATCert.

El suscriptor tiene que gestionar la firma de la hoja de entrega de poseedores de claves y la ha de custodiar durante un periodo de quince años, excepto cuando los poseedores de claves activen su certificado por medios telemáticos.

### 3.5. Poseedores de claves del suscriptor

El suscriptor se obliga a informar a los poseedores de claves de los términos y condiciones relativos al uso de los certificados.

### 3.6. Obligaciones de custodia

El suscriptor se obliga a custodiar, cuando sea preciso, el código de identificación personal, la tarjeta o cualquier otro soporte técnico entregado por CATCert, las claves privadas y, si se cabe, las especificaciones propiedad de CATCert que le sean suministradas, así como toda la información que genere en su actividad como entidad de registro.

En caso de pérdida o robo de la clave privada del certificado, o en caso de que el suscriptor sospeche que la clave privada ha perdido fiabilidad por cualquier motivo, lo tiene que notificar inmediatamente a CATCert.

### 3.7. Obligaciones de uso correcto

El suscriptor ha de utilizar el servicio de certificación prestado por CATCert, exclusivamente para los usos autorizados en la Declaración de prácticas de certificación.

El suscriptor se obliga a utilizar el servicio de certificación digital, la pareja clave pública/clave privada, la tarjeta o cualquier otro soporte técnico entregado por CATCert y los certificados de acuerdo con este convenio, y cualquier otra instrucción, manual o procedimiento suministrados por CATCert al suscriptor.

### 3.8. Transacciones prohibidas

Los servicios de certificación digital prestados por CATCert, no han sido diseñados ni permiten su utilización o reventa como equipos de control de situaciones peligrosas, o para usos que requieran actuaciones a prueba de errores, como por ejemplo la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tránsito aéreo o sistemas de control de armamento, donde un error pudiera directamente causar la muerte, daños físicos o daños medioambientales graves.

## **CUARTA. Obligaciones de CATCert**

### 4.1. Prestación del servicio de entidad de registro colaboradora

CATCert, o la entidad de registro colaboradora seleccionada por el suscriptor, tienen que registrar los datos del certificado y emitirlo posteriormente al suscriptor, por lo cual tiene que hacer las comprobaciones que considere oportunas respecto de la identidad y otras señas personales y complementarias de los suscriptores y, si se tercia, de los poseedores de claves.

Estas comprobaciones han de incluir la justificación documental aportada por la entidad de registro virtual y, si CATCert o la entidad de registro colaboradora lo consideran necesario, cualquier otro documento e información

relevante, facilitados por el subscriptor, en su caso, por el poseedor de claves, o por terceras personas.

Si CATCert o la entidad de registro colaboradora detectan errores en los datos que se han incluir en los certificados o que justifican estos datos, podrán hacer los cambios que consideren necesarios antes de emitir el certificado o parar el proceso de emisión y gestionar con el subscriptor la incidencia correspondiente.

En caso de que CATCert o la entidad de registro colaboradora corrijan los datos sin gestión previa de la incidencia correspondiente con el subscriptor, tienen que notificar los datos finalmente certificados al subscriptor, en el momento de la entrega.

CATCert se reserva el derecho a no emitir el certificado, cuando la justificación documental aportada por la entidad de registro virtual sea insuficiente para la correcta identificación y o/autenticación del subscriptor y, si cabe, del poseedor de claves.

#### 4.2. Prestación del servicio de certificación digital

CATCert se obliga a:

- a) Emitir, entregar, administrar, suspender, revocar y renovar certificados de acuerdo con las instrucciones suministradas por el subscriptor, en los casos y por los motivos descritos a la DPC de CATCert.
- b) Ejecutar los servicios con los medios técnicos y materiales adecuados, y con personal que cumpla las condiciones de cualificación y experiencia establecidas a la DPC.
- c) Cumplir los niveles de calidad del servicio, en conformidad con lo que se establece en la DPC, en los aspectos técnicos, operativos y de seguridad.
- d) Notificar al subscriptor, como mínimo con dos meses de antelación a la fecha de expiración de los certificados, la posibilidad de renovarlos, así como la suspensión, alzamiento de esta suspensión o revocación de los certificados.

- e) Comunicar a las terceras personas que lo soliciten el estado de los certificados, de acuerdo con lo que se establece en la DPC para los diferentes servicios de verificación de certificado.

## **QUINTA. Garantías**

### 5.1. Garantía de CATCert por los servicios de certificación digital

Durante la vigencia de este convenio, CATCert garantiza que la clave privada de la entidad de certificación utilizada para emitir certificados no ha sido comprometida, a no ser que CATCert no haya comunicado lo contrario mediante el registro de certificación de CATCert, de acuerdo con la Declaración de prácticas de certificación.

CATCert únicamente garantiza al subscriptor en el momento de la emisión del certificado que:

- a) Los certificados CPISR, CPX, CESR y CEX son reconocidos, en los términos previstos en la Ley 59/2003, de 19 de diciembre.
- b) CATCert no ha originado ni ha introducido declaraciones falsas o erróneas en la información de ningún certificado, ni ha dejado de incluir información necesaria aportada por la entidad de registro.
- c) Todos los certificados cumplen los requisitos formales y de contenido de la Declaración de prácticas de certificación de CATCert.
- d) CATCert ha cumplido los procedimientos descritos a la Declaración de prácticas de certificación.

CATCert aplica una diligencia razonable para asegurar que cada producto suministrado en la ejecución de este convenio es libre de cualquier virus informático, gusanos y otros códigos ilícitos, y se obliga a comunicar al subscriptor cualquier virus, gusano u otros códigos ilícitos descubiertos posteriormente en cualquier producto.

### 5.2. Exclusiones de la garantía

CATCert no garantiza ningún software que utilice el subscriptor de certificados o el poseedor de claves o cualquier otra persona para generar, verificar o utilizar de otra forma ninguna firma digital o certificado digital emitido por CATCert, excepto que haya una declaración escrita de CATCert en sentido contrario.

**SEXTA. Responsabilidad del subscriptor**

El subscriptor ha que responder ante cualquier persona por el incumplimiento de sus obligaciones del convenio y, en especial, de la actividad como entidad de registro virtual, o por negligencia, según los términos de este convenio.

El subscriptor es responsable de todas las comunicaciones electrónicas autenticadas mediante una firma digital generada con su clave privada, cuando el certificado haya sido válidamente verificado mediante los mecanismos y las condiciones establecidos por CATCert.

Mientras no se produzca la notificación establecida en el apartado 3.6 de este convenio, la responsabilidad que se pueda derivar del uso no autorizado y/o indebido de los certificados corresponde, en todo caso, al subscriptor.

**SÉPTIMA. Responsabilidad de CATCert****7.1. Responsabilidad como prestador de servicios de certificación**

CATCert tiene que responder ante de cualquier tercera persona por el incumplimiento de las obligaciones legalmente impuestas por la Ley 59/2003, de 19 de diciembre, o por negligencia, según los términos de este convenio.

CATCert no será responsable:

- a) En los casos previstos al artículo 23 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.
- b) De las informaciones contenidas en los certificados, siempre que su contenido cumpla este convenio y la DPC.
- c) De ningún daño directo o indirecto, especial, incidental o emergente; de ningún lucro cesante, pérdida de datos, daños morales o punitivos, previsibles o imprevisibles derivados del uso, distribución, licencia, funcionamiento o no funcionamiento de los certificados, las firmas digitales o cualquier transacción basada en certificados digitales, incluso aunque CATCert hubiera sido advertida de la posibilidad de la producción de los daños.

**7.2. Adecuación de los productos que hacen uso de la firma electrónica**

CATCert no se hace responsable de la adecuación de los productos y servicios relacionados con la certificación digital y la firma electrónica

existentes en el mercado que sean utilizados en aplicaciones informáticas del suscriptor, excepto cuando CATCert los suministre. En este caso, las partes quedarán sujetas a la regulación del convenio correspondiente.

Es responsabilidad del suscriptor cualquier daño derivado estrictamente de los datos y las informaciones suministradas por la institución a CATCert para la ejecución de los servicios objeto de este convenio.

#### **OCTAVA. Lugar de prestación de la actividad**

El lugar de cumplimiento de las obligaciones de CATCert relativas a los servicios de certificación digital, servicio de verificación de certificados y, en su caso, licencias de uso de software es el domicilio de CATCert, pasaje de la Concepción, 11, 08008 - Barcelona.

#### **NOVENA. Licencia de software**

CATCert concede a la institución, con carácter de no-exclusividad y intransferibilidad, licencia para utilizar las copias del software recibido de CATCert para la producción de la firma electrónica y otros servicios criptográficos por parte de los poseedores de claves.

La institución puede hacer una copia del software únicamente con el fin de archivo o copia de seguridad.

En caso de que cualquier persona diferente de CATCert haga modificaciones en el software, todas las garantías respecto al software quedarán inmediatamente canceladas.

#### **DÉCIMA. Propiedad de los certificados y las tarjetas**

Los certificados y, cuando quepa, las tarjetas de los suscriptores y de los poseedores de claves suministradas permanecen propiedad de CATCert.

CATCert se reserva el derecho discrecional de retirar o sustituir las tarjetas con certificados emitidos por CATCert por razones de seguridad, cuando queden obsoletas tecnológicamente o por cualquier otro motivo justificado.

#### **UNDÉCIMA. Uso de la imagen corporativa de las partes**

Las partes se conceden mutuamente, con carácter no exclusivo e intransferible, una licencia de uso de los diferentes elementos de su imagen

corporativa, incluyendo los signos distintivos, logotipos y marcas registradas por cada parte durante el periodo de vigencia de este convenio, exclusivamente en los materiales de marketing, publicidad, hojas de información de productos y servicios, paquetes de productos y servicios, páginas web que utilicen los productos y servicios de las partes y en las tarjetas y documentación empleadas en los procedimientos de certificación.

El uso de los elementos de la imagen corporativa de cada parte se ha de ajustar, en todo momento, al manual de imagen corporativa correspondiente, así como a las instrucciones de cada parte.

Ninguna parte concede a la otra parte ningún otro derecho sobre la marca registrada, el nombre comercial, el nombre de la empresa o las buenas prácticas comerciales de cada parte, excepto los derechos que se concretan en este convenio.

Ninguna parte puede eliminar ni destruir ninguna indicación relativa a los derechos de autor, las patentes o las marcas comerciales contenidos en cualquier producto, servicio electrónico o documentación de todo tipo.

#### **DUODÉCIMA. Protección de las señas personales**

CATCert es titular de un conjunto de ficheros de datos de carácter personal relativos a los datos de identificación y autenticación de los usuarios de los servicios de certificación digital, tal y como se especifica en la Declaración de prácticas de certificación de CATCert.

CATCert capta las señas personales que figuran en los ficheros por varios procedimientos:

- a) Por cesión de los datos por parte del suscriptor, que las ha de haber obtenido legalmente, en las condiciones previstas a la normativa sobre firma electrónica y sobre protección de datos de carácter personal.
- b) Con la colaboración de entidades públicas, que actúan como entidades de registro colaboradoras de certificados de clase 1
- c) Directamente de los poseedores de claves, cuando el registro de sus datos es excepcionalmente efectuado por CATCert.

CATCert se obliga a cumplir la normativa sobre firma electrónica y sobre protección de datos de carácter personal, en especial con respecto a la inscripción y la correcta gestión de los ficheros de datos personales, con las medidas de seguridad correspondientes.

La institució queda lliurada de qualsevol responsabilitat derivada del dany ocasionat per les incidències produïdes de la gestió de les dades de caràcter personal cedides a CATCert.

### **DECIMOTERCERA. Resolució del conveni**

La resolució del conveni tindrà lloc en els casos següents:

- a) Por incumplimiento: las partes tienen derecho a resolver este convenio en el supuesto de incumplimiento por la otra parte de cualquiera de sus obligaciones, si esta infracción no ha sido solucionada:
  - a. Dentro de los treinta días desde la recepción de la notificación efectuada por la parte que no ha dejado de cumplir sus obligaciones.
  - b. Inmediatamente, si el incumplimiento compromete la seguridad de los servicios.
- b) Por concurrencia de cualquier otra causa de resolución anticipada establecida por la legislación vigente y, especialmente, por la legislación vigente de firma electrónica y certificación digital.