INFRAESTRUCTURA DE FIRMA DIGITAL – REPÚBLICA ARGENTINA

LEY Nº 25.506

TÉRMINOS Y CONDICIONES CON TERCEROS USUARIOS

AC ONTI

DIRECCIÓN NACIONAL DE TRAMITACIÓN E IDENTIFICACIÓN A DISTANCIA

SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA

SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA

SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN

JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN

Versión 3.0

Enero 2019

ÍNDICE

1. INTRODUCCIÓN.

El presente documento establece los términos y condiciones que rigen la relación entre el Certificador Licenciado y los Terceros Usuarios en lo que respecta a los certificados digitales emitidos por la Autoridad Certificante de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (en adelante, AC ONTI) de acuerdo con los términos de la "Política Única de Certificación" y determina los derechos y responsabilidades de las partes en relación a la verificación de firmas digitales y aplicabilidad de dichos certificados digitales.

2. RESUMEN.

Por el presente, los Terceros Usuarios que verificarán los certificados digitales toman conocimiento y aceptan que el Certificador no tiene vínculo contractual alguno con ellos y se limitarán a utilizar los servicios del repositorio público actualizado por la AC ONTI en el marco de la "Política Única de Certificación", de acuerdo con la normativa vigente.

Resultan aplicables la Ley Nº 25.506 de Firma Digital, su Decreto Reglamentario Nº 2628/02, el Decreto N° 892/2017, la Resolución Nº 399-E/16 del entonces MINISTERIO DE MODERNIZACIÓN y modificatorias; la "Política Única de Certificación" y la documentación de la AC ONTI relacionada con su correspondiente licencia, la que se encuentra publicada en el sitio web de la AC ONTI.

3. DEFINICIONES.

AUTORIDAD CERTIFICANTE (AC): Es el componente de la Infraestructura Tecnológica del Certificador que emite certificados digitales a los suscriptores de certificados emitidos en base a la "Política Única de Certificación", las funciones de Autoridad Certificante son ejercidas por la AC ONTI.

AUTORIDAD DE REGISTRO (AR): Es la entidad que tiene a su cargo las funciones indicadas en artículo 35 del Decreto Nº 2628/02.

CERTIFICADO DIGITAL: Se entiende por certificado digital al documento digital firmado digitalmente por un certificador licenciado, que vincula los datos de verificación de firma a su titular (art. 13 ley N° 25.506).

CERTIFICADOR LICENCIADO: Se entiende por Certificador Licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante (Artículo 17 de la Ley N° 25.506).

LISTA DE CERTIFICADOS REVOCADOS (CRL): Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés: *Certificate Revocation List* (CRL). (Anexo I del Decreto 2628/02).

OCSP (PROTOCOLO EN LÍNEA DEL ESTADO DE UN CERTIFICADO – "*ONLINE CERTIFICATE STATUS PROTOCOL*"): Servicio de verificación en línea del estado de los certificados. El OCSP es un método para determinar el estado de revocación de un certificado digital usando otros medios que no sean el uso de Listas de

Revocación de Certificados (CRL). El resultado de una consulta a este servicio está firmado por la AC ONTI que brinda el servicio.

MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN (CPS): Conjunto de prácticas utilizadas por la AC ONTI en la emisión y administración de los certificados. En inglés: *Certification Practice Statement* (CPS). (Anexo I del Decreto N° 2628/02).

POLÍTICA DE CERTIFICACIÓN (CP): Conjunto de criterios que indican la aplicabilidad de un certificado digital a un grupo de usuarios en particular o a un conjunto de aplicaciones con similares requerimientos de seguridad (Anexo I del Decreto N° 2628/02).

REPOSITORIO: Sitio web donde los terceros usuarios, los suscriptores, otros interesados y el público en general, pueden obtener información relacionada con el Certificador Licenciado y su Política de Certificación. En el repositorio están disponibles el certificado de la AC ONTI (emitido por la Autoridad Certificante Raíz de la República Argentina), su Política Única de Certificación, su Manual de Procedimientos, la Lista de Certificados Revocados, el “Acuerdo con Suscriptores”, los “Términos y Condiciones con Terceros Usuarios”, la “Política de Privacidad” y toda otra información considerada de naturaleza pública por el propio Certificador.

SUSCRIPTOR O TITULAR DE UN CERTIFICADO DIGITAL: Persona a cuyo nombre se emite un certificado digital y posee una clave privada que se corresponde con la clave pública contenida en el mismo, también son titulares las aplicaciones o sitios web a nombre de los cuales se emite un certificado digital.

SOLICITANTE DE UN CERTIFICADO DIGITAL: Persona humana que solicita un certificado digital a un Certificador Licenciado.

TERCERO USUARIO: persona humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente, de acuerdo al Anexo I del Decreto N° 2628 del 19 de diciembre de 2002 y modificatorios.

4. RECONOCIMIENTO DE INFORMACIÓN SUFICIENTE.

El Tercero Usuario cuenta con información suficiente disponible en el repositorio público que se encuentra en la URL (https://pki.jgm.gov.ar/app/), accesible VEINTICUATRO (24) horas los SIETE (7) días de la semana, cuyo detalle se encuentra en el punto 2.2 “Publicación de información de la AC ONTI” de la Política Única de Certificación. El Tercero Usuario acepta su obligación de conocer la “Política Única de Certificación” y los “Términos y Condiciones con Terceros Usuarios”. Para la verificación de la vigencia del certificado digital se podrá consultar los sitios de Internet habilitados por el certificador con ese fin y utilizar los medios disponibles tales como la consulta en línea del estado de los certificados (OCSP) o la CRL. Esta verificación debe extenderse hasta el certificado digital de la Autoridad Certificante Raíz de la República Argentina.

5. POLÍTICA DE CERTIFICACIÓN.

5.1. TIPOS DE CERTIFICADOS.

La AC ONTI emite los siguientes tipos de certificados digitales

a) Para Personas Humanas
b) Para Autoridad de Sello de tiempo
c) Para Aplicaciones
d) Para OCSP, usado en el servicio de verificación en línea del estado de un certificado.

La Política Única de Certificación contempla y define un Nivel de Seguridad Alto para los certificados emitidos a favor de sus suscriptores de certificados de personas humanas. Las claves criptográficas de los suscriptores de certificados de personas humanas son generadas por hardware (ej: tokens, smartcards) y almacenadas por ellos.

De acuerdo a lo indicado en el punto 1.3.3 de la Política Única de Certificación de la AC ONTI, podrán ser suscriptores de los certificados emitidos por la AC ONTI las personas humanas que requieran un certificado digital para firmar digitalmente cualquier documento o transacción, pudiendo ser utilizados para cualquier uso o aplicación, como así también para autenticación o cifrado.

La AC ONTI emite también un certificado para ser usado en relación con el *servicio On Line Certificate Status Protocol* (en adelante, OCSP) de consulta sobre el estado de un certificado.

Asimismo, la AC ONTI emite certificados de aplicación y presta el servicio de sello de tiempo, según lo dispuesto en el artículo 9° de la Resolución MM N° 399-E/2016 del 5 de octubre de 2016 del entonces MINISTERIO DE MODERNIZACIÓN.

.

5.2. APLICABILIDAD.

Las claves correspondientes a los certificados digitales que se emitan bajo la Política Única de Certificación de la AC ONTI podrán ser utilizadas en forma interoperable en los procesos de firma digital de cualquier documento o transacción y para la autenticación o el cifrado.

5.3. LIMITACIONES EN EL USO DE LOS CERTIFICADOS.

No existen limitaciones en cuanto al uso que el suscriptor quiera darle al certificado digital excepto aquellos establecidos en la normativa vigente.

6. OBLIGACIONES DEL TERCERO USUARIO (“relying party”).

Las obligaciones de los Terceros Usuarios son:

a) Conocer los alcances de la “Política Única de Certificación”.

b) Verificar la validez del certificado digital.

7. REVOCACIÓN DE LOS CERTIFICADOS DE NIVEL SUPERIOR.

El Tercero Usuario acepta su responsabilidad en cuanto al control de la validez de toda la cadena de certificados que intervienen en la firma digital que deba verificar, incluyendo el certificado digital de la Autoridad Certificante Raíz de la República Argentina (AC Raíz de la RA). En el caso en que alguno de los certificados hubiera sido revocado o hubiera expirado a la fecha de la firma del documento, la firma digital carecerá de validez.

En caso de producirse la revocación de los certificados de nivel superior, este estado se hará evidente para el Tercero Usuario en el momento en que genere una consulta para verificar la validez del certificado digital de un suscriptor. La validez del certificado de un suscriptor se comprueba mediante un procedimiento de verificación de su cadena de confianza, el cual se realiza en el siguiente orden:

a) Contra el certificado digital con que se firmó el documento.
b) Contra el certificado digital correspondiente a la AC que emitió el certificado del suscriptor, es decir el certificado de la AC ONTI.
c) Contra el certificado digital correspondiente a la AC que emitió el certificado de la AC ONTI, es decir, el certificado de la AC Raíz de la REPÚBLICA ARGENTINA.

Estas verificaciones se realizarán utilizando las CRLs correspondientes a cada Autoridad Certificante mencionada**,** o contra su servicio OCSP de corresponder.

8. LIMITACIONES DE RESPONSABILIDAD.

El Certificador no asumirá responsabilidad alguna en aquellos supuestos que se excluyan taxativamente en las condiciones de emisión de sus certificados, por los daños y perjuicios que resultaren del uso no autorizado de un certificado digital y por eventuales inexactitudes contenidas en el certificado que resulten de la información facilitada por el titular, conforme lo establece el artículo 39 de la Ley 25.506

8.1. FUERZA MAYOR.

Conforme a lo dispuesto por el artículo 1730 del Código Civil y Comercial de la Nación, no generarán derecho a indemnización a favor del damnificado aquellas causas que siendo ajenas a la voluntad de las partes, no se puedan evitar y tampoco se puedan prever. Para ello, la parte que las invocare deberá poner en conocimiento de la otra parte, de manera fehaciente, las circunstancias del hecho, dentro de las VEINTICUATRO (24) horas de conocidas y siempre que haya tomado las medidas que resulten razonablemente necesarias, para mitigar los efectos ocasionados por el hecho de fuerza mayor invocado.

8.2. CASOS EN LOS CUALES EL CERTIFICADOR PUEDE LIMITAR SU RESPONSABILIDAD.

De acuerdo con lo estipulado en el art 39 de la Ley Nº 25.506, el Certificador no será responsable:

a) Por los casos en que los certificados se utilicen para aplicaciones distintas a las detalladas en el apartado “5.2.- Aplicabilidad” del presente documento.
b) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y aquellos que no estén expresamente previstos en la ley.
c) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización.
d) Por las eventuales inexactitudes en el certificado digital que resulten de la información facilitada por el suscriptor que, según lo dispuesto en las normas

y en los manuales de procedimientos respectivos, deba ser objeto de verificación siempre que la AC ONTI pueda demostrar que ha tomado todas las medidas razonables.

9. LEGISLACIÓN APLICABLE Y PROCEDIMIENTOS DE RESOLUCIÓN DE CONFLICTOS.

El presente documento, la “Política Única de Certificación”, su correspondiente Manual de Procedimientos y demás documentos aprobados durante el proceso de licenciamiento se encuentran sometidos a lo establecido por la Ley N° 25.506, su Decreto Reglamentario N° 2628/02, la Resolución MM N° 399-E/2016 del ex MINISTERIO DE MODERNIZACIÓN, el Decreto N° 892/2017 y demás normas complementarias dictadas por la Autoridad de Aplicación y el Ente Licenciante.

Cualquier controversia y/o conflicto resultante de la aplicación de los documentos antes mencionados, deberá ser resuelta en sede administrativa de acuerdo a las previsiones de la Ley Nacional de Procedimientos Administrativos N° 19.549 y su Decreto Reglamentario N° 1759/72 T.O. 2017.

Los Terceros Usuarios podrán interponer ante el Ente Licenciante recurso administrativo por conflictos referidos a la prestación del servicio por parte del Certificador previo reclamo ante la AC ONTI.

Una vez agotada la vía administrativa, podrá interponerse acción judicial, siendo competente al respecto la Justicia en lo Contencioso Administrativo Federal.

El reclamo efectuado por un tercero usuario respecto a un certificado digital expedido por la AC ONTI, sólo será procedente, previa acreditación de haberse

efectuado reclamo previo ante la referida Autoridad Certificante con resultado negativo. Acreditada dicha circunstancia, el Ente Licenciante procederá a recibir, evaluar y resolver las denuncias mediante la instrucción del correspondiente trámite administrativo.

10. CONTACTOS.

Los Terceros Usuarios podrán contactarse con el Certificador Licenciado por:

Correo electrónico: consultapki@modernizacion.gob.ar

Historia de las revisiones:

Versión y Modificación	Fecha de emisión	Descripción	Motivo del Cambio
Versión 1.1	09/2010	Nuevo documento	Licenciamiento AC ONTI
Versión 2.0	08/2015	Actualización	Adecuación DA 927/2014
Versión 3.0	01/2019	Actualización	Actualización documentación AC ONTI

Nota: Cada nueva versión y/o modificación suplanta a las anteriores, resultando sólo vigente la última, la que está representada por el presente documento.

República Argentina - Poder Ejecutivo Nacional
2019 - Año de la Exportación

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2019-01737683-APN-DNTEID#JGM

CIUDAD DE BUENOS AIRES
Miércoles 9 de Enero de 2019

Referencia: Términos y Condiciones con Terceros Usuarios AC ONTI v3.0

El documento fue importado por el sistema GEDO con un total de 12 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=MINISTERIO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2019.01.09 21:24:54 -03'00'

Alejandra Battaglia
Directora Nacional
Dirección Nacional de Tramitación e Identificación a Distancia
Jefatura de Gabinete de Ministros

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=MINISTERIO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2019.01.09 21:24:55 -03'00'