



Jefatura de Gabinete de Ministros
Secretaría de Gabinete
Subsecretaría de Tecnologías de Gestión

ANEXO III

Infraestructura de Firma Digital – REPÚBLICA ARGENTINA

Ley N° 25.506

TÉRMINOS Y CONDICIONES CON TERCEROS USUARIOS

POLÍTICA ÚNICA DE CERTIFICACIÓN de la AC ONTI

Versión 2.0



OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN
SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN
SECRETARÍA DE GABINETE
JEFATURA DE GABINETE DE MINISTROS



Jeftura de Gabinete de Ministros
Secretaría de Gabinete
Subsecretaría de Tecnologías de Gestión

ANEXO III

ÍNDICE

1. RESUMEN	3
2. DEFINICIONES.....	3
3. RECONOCIMIENTO DE INFORMACIÓN SUFICIENTE.....	5
4. POLÍTICA DE CERTIFICACIÓN	6
4.1. TIPOS DE CERTIFICADOS	6
4.2. APLICABILIDAD	7
4.3. LIMITACIONES EN EL USO DE LOS CERTIFICADOS.....	7
5. OBLIGACIONES DEL TERCERO USUARIO ("relying party")	7
6. REVOCACIÓN DE LOS CERTIFICADOS DE NIVEL SUPERIOR	7
7. LIMITACIONES DE RESPONSABILIDAD	8
7.1. FUERZA MAYOR	9
7.2. CASOS EN LOS CUALES EL CERTIFICADOR PUEDE LIMITAR SU RESPONSABILIDAD	9
8. LEGISLACIÓN APLICABLE Y PROCEDIMIENTOS DE RESOLUCIÓN DE CONFLICTOS.....	10
9. CONTACTOS	11



Jefatura de Gabinete de Ministros
Secretaría de Gabinete
Subsecretaría de Tecnologías de Gestión

ANEXO III

1. RESUMEN.

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 ONTI (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.

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 N° 25.506 de Firma Digital, su Decreto Reglamentario N° 2628/02, la Decisión Administrativa N° 927/2014 de la Jefatura de Gabinete de Ministros; la "Política Única de Certificación" y la documentación del Certificador relacionada con su correspondiente licencia, la que se encuentra publicada en el sitio web de la AC ONTI.

2. DEFINICIONES.

- TERCERO USUARIO: es la persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente (art. 3° del Decreto N° 724/06).
- CERTIFICADO DIGITAL: Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (art. 13 ley N° 25.506).



*Jefatura de Gabinete de Ministros
 Secretaría de Gabinete
 Subsecretaría de Tecnologías de Gestión*

ANEXO III

- **POLÍTICA DE CERTIFICACIÓN (PC):** 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 2628/02).
- **MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN (MPC):** Conjunto de prácticas utilizadas por el Certificador Licenciado en la emisión y administración de los certificados (Anexo I del Decreto 2628/02).
- **LISTA DE CERTIFICADOS REVOCADOS (LCR):** 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 (Anexo I del Decreto 2628/02).
- **SUSCRIPTOR O TITULAR DE UN CERTIFICADO DIGITAL:** Persona o entidad a cuyo nombre se emite un certificado digital y posee una clave privada que se corresponde con la clave pública contenida en el mismo.
- **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 25.506).
- **AUTORIDAD DE REGISTRO (AR):** es la entidad que tiene a su cargo las funciones de:
 - Recepción de las solicitudes de emisión de certificados.
 - Validación de la identidad y autenticación de los datos de los titulares de certificados.



Jefatura de Gabinete de Ministros
Secretaría de Gabinete
Subsecretaría de Tecnologías de Gestión

ANEXO III

- Validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado.
- Remisión de las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.
- Recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado con el que se vinculen.
- Identificación y autenticación de los solicitantes de revocación de certificados.
- Archivo y la conservación de toda la documentación de respaldo del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.
- Cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
- Cumplimiento de las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.

Dichas funciones son delegadas por el certificador licenciado. Puede actuar en una instalación fija o en modalidad móvil, siempre que medie autorización del ente licenciante.

3. 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



Jefatura de Gabinete de Ministros
Secretaría de Gabinete
Subsecretaría de Tecnologías de Gestión

ANEXO III

"Publicación de información del Certificador". 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.

4. POLÍTICA DE CERTIFICACIÓN.

4.1. TIPOS DE CERTIFICADOS.

La AC ONTI emite los siguientes tipos de certificados digitales, de acuerdo a lo indicado en el punto 1.3.3 de la "Política Única de Certificación":

- a) Para Personas Físicas que desempeñen funciones en entes públicos estatales;
- b) Para Personas Físicas o Jurídicas que realicen trámites con el Estado, cuando existe una aplicación que requiera una firma digital;
- c) Para organismos y empresas públicas;
- d) Para OCSP, cuyo suscriptor es la Oficina Nacional de Tecnologías de Información, usado en el servicio de verificación en línea del estado de un certificado;
- e) Para Proveedores de servicios en relación a la firma digital.

La presente Política contempla y define dos niveles de seguridad para los certificados emitidos a favor de sus suscriptores (excluidos certificados OCSP):



Jefatura de Gabinete de Ministros
Secretaría de Gabinete
Subsecretaría de Tecnologías de Gestión

ANEXO III

- a) Nivel de seguridad Alto: para los certificados solicitados mediante el uso de dispositivos criptográficos (ej: tokens, smart cards).
- b) Nivel de seguridad Normal: correspondiente a los certificados solicitados y almacenados vía software.

4.2. APLICABILIDAD.

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

4.3. LIMITACIONES EN EL USO DE LOS CERTIFICADOS.

No existen restricciones excepto las que surgen del punto anterior.

5. 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.

6. 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



*Jefatura de Gabinete de Ministros
 Secretaría de Gabinete
 Subsecretaría de Tecnologías de Gestión*

ANEXO III

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 de la 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 RA.

Estas verificaciones se realizarán utilizando las CRLs correspondientes a cada Autoridad Certificante mencionada.

7. LIMITACIONES DE RESPONSABILIDAD.

Las responsabilidades y garantías para el Certificador licenciado, sus AR, los suscriptores, los terceros usuarios y otras entidades participantes, se originan en lo establecido por la Ley N° 25.506 y su Decreto Reglamentario N° 2628/02 y en las disposiciones de la Política Única de Certificación.

Las limitaciones de responsabilidad del Certificador Licenciado respecto a otras entidades participantes, se rigen por lo establecido en el art. 39 de la Ley N° 25.506, en las disposiciones de la presente Política y en los Términos y Condiciones con terceros usuarios.



Jefatura de Gabinete de Ministros
Secretaría de Gabinete
Subsecretaría de Tecnologías de Gestión

ANEXO III

7.1. FUERZA MAYOR.

Conforme a lo dispuesto por el artículo 514 del Código Civil de la Nación (actualmente vigente) y el artículo 1730 del Código Civil y Comercial de la Nación (que entrará en vigencia a partir del 1º de agosto de 2015), 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 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.

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

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

- a) 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.
- b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital.
- c) 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 el Certificador pueda demostrar que ha tomado todas las medidas razonables.



Jefatura de Gabinete de Ministros
Secretaría de Gabinete
Subsecretaría de Tecnologías de Gestión

ANEXO III

8. 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 25.506, su Decreto Reglamentario 2628/02 y la Decisión Administrativa N° 927/14 y demás normas complementarias dictadas por la Autoridad de Aplicación.

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.

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 de dicho Certificador.

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.



Jefatura de Gabinete de Ministros
Secretaría de Gabinete
Subsecretaría de Tecnologías de Gestión

ANEXO III

9. CONTACTOS.

Los Terceros Usuarios podrán contactarse con el Certificador:

OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN

Domicilio: Roque Sáenz Peña 511 - 5° piso (C1035AAA) Ciudad Autónoma de Buenos Aires

Argentina

Correo electrónico: aconti@jefatura.gob.ar

Teléfonos: (54 11) 5985-8663

(54 11) 4343-9001 Int. 533



*Jefatura de Gabinete de Ministros
 Secretaría de Gabinete
 Subsecretaría de Tecnologías de Gestión*

ANEXO III

Historia de las revisiones:

Versión y Modificación	Fecha de emisión	Descripción	Motivo del Cambio
Versión 1.1	23/09/2010		Actualización
Versión 2.0	01/05/2014		

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