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

ANEXO II

Infraestructura de Firma Digital – REPÚBLICA ARGENTINA

Ley Nº 25.506

ACUERDO CON SUSCRIPTORES

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

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

ANEXO II

ÍNDICE

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

ANEXO II

ACUERDO CON SUSCRIPTORES

El presente acuerdo entre la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (en adelante ONTI) y el suscriptor de un certificado digital emitido por la Autoridad Certificante de la ONTI (en adelante AC ONTI) determina los derechos y obligaciones de la partes respecto a la solicitud, aceptación y uso de los certificados emitidos en el marco de la Política Única de Certificación.

1. SOLICITUD DE CERTIFICADO Y DESCRIPCIÓN DE LOS CERTIFICADOS.

Podrán ser suscriptores de los certificados emitidos por la AC ONTI los funcionarios, agentes públicos y las personas contratadas bajo cualquier modalidad de contratación que desempeñen funciones en los organismos y entidades del Sector Público.

Podrán también ser suscriptores de los certificados emitidos por la AC ONTI, los particulares que realicen trámites electrónicos para los que el Sector Público requiera una firma digital.

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.

La Política Única de Certificación correspondiente a la AC ONTI contempla dos niveles de seguridad para los certificados emitidos a favor de sus suscriptores:

- Nivel de seguridad Alto: para los certificados solicitados cuyas claves privadas fueron generadas y almacenadas en dispositivos criptográficos (ej: tokens, smart cards) FIPS 140-2 Nivel 2.

ANEXO II

- Nivel de seguridad Normal: correspondiente a los certificados cuyas claves privadas fueron generadas y almacenados vía software.

2. PROCESAMIENTO DE LA SOLICITUD DE CERTIFICADO DEL SUSCRIPTOR.

El proceso de solicitud puede ser iniciado solamente por el interesado, quien posteriormente debe acreditar fehacientemente su identidad, presentando la documentación prevista en los apartados 3.2.3. - Autenticación de la identidad de Personas Físicas de la Política Única de Certificación, así como la constancia de C.U.I.T. o C.U.I.L. Deberá también demostrar la pertenencia a la comunidad de suscriptores prevista en el apartado 1.1 del presente acuerdo.

Los pasos para realizar la solicitud son los siguientes:

a) Ingresar al sitio web del Certificador https://pki.jgm.gob.ar/app/ seleccionando el enlace a la aplicación de solicitud de emisión de certificados.
b) Completar la solicitud de certificado con los datos requeridos, seleccionando la AR que le corresponde luego de seleccionar si genera sus claves por software (nivel de seguridad normal) o utilizando un dispositivo criptográfico (nivel de seguridad alto).
c) Aceptar el presente Acuerdo con Suscriptores.
d) Enviar su solicitud a la AC ONTI, imprimirla y firmarla.
e) Presentarse ante la AR correspondiente para realizar la identificación personal y la verificación de la documentación requerida.

ANEXO II

En el caso de funcionarios, agentes o personas contratadas en el Sector Público, se aceptará únicamente como dirección de correo electrónico válida aquella que revista carácter institucional y se encuentre accesible por un cliente de correo electrónico.

En el caso que se utilicen dispositivos criptográficos, estos deberán cumplir con la certificación de NIST FIPS 140-2 Nivel 2, como mínimo. Los suscriptores generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 2048 bits.

El par de claves del suscriptor de un certificado digital debe ser generado de manera tal que su clave privada se encuentre bajo su exclusivo y absoluto control. El suscriptor es considerado titular del par de claves; como tal, está obligado a generarlas en un sistema confiable y a no revelar su clave privada a terceros bajo ninguna circunstancia.

La clave pública del solicitante es entregada a la aplicación de la AC ONTI durante el proceso de solicitud de certificado utilizando técnicas de "prueba de posesión" de la clave privada asociada.

Los procesos de solicitud utilizan el formato PKCS#10 para implementar la "prueba de posesión", remitiendo los datos del solicitante y su clave pública dentro de una estructura firmada con su clave privada.

La documentación suministrada por el solicitante y/o suscriptor durante el procedimiento de identificación y autenticación de la identidad culminó con la emisión del certificado digital por parte de la AC ONTI.

3. OBLIGACIONES ANTE LA REVOCACIÓN O EXPIRACIÓN.

Los suscriptores de los certificados digitales asumen las siguientes obligaciones:

ANEXO II

- Mantener el control exclusivo de los datos de creación de su firma digital, no compartirlos, e impedir su divulgación;
- Utilizar un dispositivo de creación de firma digital que cumpla con las características definidas en la Política Única de Certificación en caso de corresponder;
- Solicitar la revocación de su certificado al Certificador ante cualquier circunstancia que pudiere comprometer la privacidad de sus datos de creación de firma;
- Informar sin demora al Certificador el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación;
- Revocar su Certificado en caso de producirse cualquier modificación de los datos contenidos en el mismo.
- Proveer toda la información que le sea requerida a los fines de la emisión del certificado de modo completo y preciso;
- Utilizar los certificados de acuerdo con los términos y condiciones establecidos en la Política Única de Certificación que respalde su emisión;
- Verificar la exactitud de los datos contenidos en su certificado al momento de su entrega;

El Certificador asume las obligaciones establecidas en la Política Única de Certificación, el Manual de Procedimientos de Certificación, la Política de Privacidad, la Política de Seguridad y la restante documentación publicada, conforme la Ley N° 25.506, su normativa reglamentaria y complementaria.

ANEXO II

4. POLÍTICA DE PRIVACIDAD.

El Certificador cumplirá con lo establecido en su documento de Política de Privacidad, publicado en su sitio Web, protegiendo así los datos, tanto de los suscriptores como los propios. Mediante el presente acuerdo, el suscriptor manifiesta conocer y aceptar los términos de dicha Política.

5. LIMITACIONES DE LA RESPONSABILIDAD.

El Certificador no asumirá responsabilidad alguna en aquellos supuestos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados, en los supuestos de daños y perjuicios que resultaren del uso no autorizado de un certificado digital y en los supuestos donde las inexactitudes contenidas en el certificado resultaran de la información que hubiera presentado el suscriptor.

5.1 - Fuerza mayor.

Las partes del presente acuerdo no serán consideradas como responsables o incumplidoras, por cualquier finalización, interrupción o demora en el cumplimiento de sus obligaciones, que resultara como consecuencia de un terremoto, inundación, incendio, vendaval, desastre natural, guerra, conflicto armado, acción terrorista, siempre y cuando la parte que invoca esta sección haya puesto esta circunstancia en conocimiento de la otra parte dentro de los cinco (5) días de conocido el fenómeno, y que haya tomado oportunamente las medidas necesarias para mitigar los efectos ocasionados por el hecho de fuerza mayor alegado.

ANEXO II

5.2 - Casos en los cuales el certificador puede limitar o eximirse de su responsabilidad.

El Certificador sólo asumirá las responsabilidades expresamente establecidas en la Ley Nº 25.506, sus normas reglamentarias y complementarias, eximiéndose de todo tipo de responsabilidad civil, penal, comercial, entre otras, por cualquier circunstancia o casos en que se hubiera utilizado de forma indebida un certificado que contenga inexactitudes en los datos contenidos, que resulten de información facilitada por el suscriptor.

6. LEY Y JURISDICCIÓN APLICABLE Y PROCEDIMIENTO DE RESOLUCIÓN DE CONFLICTOS.

La Política Única de Certificación, su correspondiente Manual de Procedimientos se encuentran sometidos a lo establecido por la Ley N° 25.506, su Decreto Reglamentario N° 2628/02, la Decisión Administrativa N° 927/2014 y demás normas complementarias dictadas por la Autoridad de Aplicación.

Cualquier controversia y/o conflicto resultante de la aplicación de la Política de Única de Certificación, 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.

La presente Política Única de Certificación se encuentra en un todo subordinada a las prescripciones de la Ley N° 25.506 y su reglamentación.

Los titulares de certificados y los terceros usuarios podrán interponer ante el Ente Licenciante recurso administrativo por conflictos referidos a la prestación del servicio por

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

El reclamo efectuado por un tercero usuario o por el titular de un certificado digital expedido por la AC ONTI, sólo será procedente previa acreditación de haberse efectuado reclamo previo ante esta última con resultado negativo. Acreditada dicha circunstancia, el Ente Licenciante procederá a recibir, evaluar y resolver las denuncias mediante la instrucción del correspondiente trámite administrativo.

7. CESIÓN DE DERECHOS.

Ninguna de las obligaciones del suscriptor de un certificado digital bajo el presente acuerdo podrá ser cedida o transferida.

8. DECLARACIÓN JURADA.

El suscriptor declara que la información contenida en el certificado digital es fidedigna.

El suscriptor declara haber leído y aceptado en todos sus términos la Política Única de Certificación de la AC ONTI.

9. CONTACTOS.

Los suscriptores de los certificados de la AC ONTI, a los efectos de toda consulta, sugerencia y tramitación, deberán dirigirse a:

OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN

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

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

ANEXO II

Por correo electrónico: contactopki@jefatura.gob.ar

Teléfono: (54 11) 4343-9001 Int. 533 o 5985-8663

10. VIGENCIA.

El solicitante de un certificado digital, una vez cumplidos los requisitos definidos por el Certificador, deberá aceptar el presente Acuerdo, el que declara conocer y aceptar en todos sus términos y condiciones, como así también el marco normativo aplicable: la Ley Nº 25.506, el Decreto N° 2628/2002, la Decisión Administrativa Nº 927/2014, la Disposición Nº 11/2014 de la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN que aprueba la adhesión de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN, en su calidad de Certificador Licenciado, a la "Política Única de Certificación"; y demás normas complementarias.

El presente acuerdo comenzará a regir a partir de la fecha de emisión del certificado digital a favor del suscriptor, siempre y cuando no haya incurrido en incumplimiento de las obligaciones contraídas como tal, durante el período de vigencia de dicho certificado, quedando limitado a la vigencia del certificado de la AC ONTI, el cual no podrá ser excedido en un período mayor por el certificado del suscriptor.

11. MODIFICACIÓN A ESTE ACUERDO.

El Certificador se reserva el derecho exclusivo de modificar el presente acuerdo, previa revisión y aprobación del Ente Licenciante. Cualquier cambio en sus especificaciones dará lugar a la firma de un nuevo acuerdo con cancelación del presente.

ANEXO II

Historia de las revisiones:

Versión y Modificación	Fecha de emisión	Descripción	Motivo del Cambio

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