



Ciudad Autónoma de Buenos Aires, 01 JUN. 2016

VISTO:

La Constitución Local, la Ley N° 3 de la Ciudad Autónoma de Buenos Aires, el Reglamento Interno de Organización y Funcionamiento de esta Defensoría del Pueblo, el Convenio suscripto con el Ministerio de Modernización de la Ciudad, la implementación del uso de nuevas tecnologías para la administración y la necesidad de brindar un cauce orgánico a la implementación de la Firma Digital (FD) y las Comunicaciones Oficiales (CCOO) de esta Defensoría del Pueblo.

Y CONSIDERANDO QUE:

El artículo 137 de la Constitución de la Ciudad Autónoma de Buenos Aires crea a esta Defensoría del Pueblo como organismo con autonomía funcional y autarquía financiera.

El inciso g) del artículo 4° del Reglamento Interno de Organización y Funcionamiento Institucional, dota con carácter exclusivo al Defensor del Pueblo entre otras competencias y atribuciones la de: *"aprobar los procedimientos administrativos que regulan el desenvolvimiento institucional"*

El inciso i) del mismo Reglamento lo faculta a: *"aprobar la implementación de los sistemas informáticos y el diseño de aquellos que se desarrollen internamente en la Institución"*.

El artículo 14 del Reglamento establece, entre otros, como principios rectores del modelo de gestión a implementar: *"la legalidad, la eficacia, la eficiencia, la agilidad y transparencia administrativa, la coordinación, cooperación y trabajo transversal de los órganos a cargo"* para el cumplimiento de sus fines.

Por su parte el artículo 16 al referirse sobre la informatización indica que la Defensoría del Pueblo *"facilita la progresiva optimización de esas*

herramientas con la finalidad puesta en la mejora del servicio al ciudadano y de la propia gestión interna. En ese sentido, debe promover la facilitación y simplificación de las modalidades de acceso y realización de trámites, el intercambio documental y de información desde y hacia el ciudadano, y como herramienta para la administración interna de la organización”.

Asimismo, de conformidad con los principios de la “*Carta Iberoamericana de Calidad en la Gestión Pública*”, esta Defensoría concibe que la calidad institucional atañe –entre otras cuestiones- a la racionalización del gasto, la generación de una cultura transformadora, el impulso de la mejora permanente, y la eficacia y eficiencia en el uso de los recursos públicos. En esa línea, promueve la agilización y simplificación de los trámites administrativos como un desafío permanente.

El uso de estas nuevas tecnologías, no agota su resultado en sí mismo, sino que tiene un efecto expansivo sobre el rol institucional de las distintas administraciones, proveyendo un mejor y más accesible servicio al ciudadano.

A su vez, la aplicación de las nuevas tecnologías al Derecho Administrativo plantea dos retos: uno tecnológico y uno jurídico. El reto tecnológico consiste en crear programas y sistemas que se adecuen a las exigencias constitucionales, legales y, en general, normativas que caracterizan al Derecho Administrativo, ámbito en el que van a ser aplicados; el reto jurídico consiste en establecer tales exigencias (adaptar en algunos casos, crear en otros) en el marco de las nuevas tecnologías y en determinar el régimen jurídico de su aplicación.

La implementación de estas tecnologías supone el dictado de un marco normativo, que dote a las nuevas herramientas y tecnologías a utilizar, de las garantías y principios jurídicos que el Derecho Administrativo concibe y otorga, para el correcto desarrollo de los fines de todo actuar administrativo.

La utilización de Firma Digital y Firma Electrónica permitirá el manejo de los documentos y de la información, mediante el empleo de soluciones integradas, comunes, compatibles y coordinadas. La incorporación de estas tecnologías a



nuestra práctica administrativa constituye un elemento superador que parte de una visión integrada de la gestión administrativa, enmarcada en el compromiso de esta gestión con el proceso de mejora y desarrollo institucional, lo que involucra necesariamente su implementación progresiva.

Así, resulta necesario establecer que las comunicaciones internas de carácter administrativo que mantienen los sectores de esta Institución entre sí se efectúen a través del módulo de "Comunicaciones Oficiales".

Resulta innegable la conveniencia de impulsar en el ámbito de esta Defensoría del Pueblo la Ciudad Autónoma de Buenos Aires el uso de este tipo de herramientas tecnológicas, en un marco dispositivo que regule jurídicamente su utilización.

En base a ello, el dictado de la presente Disposición resulta necesaria a efectos de dotar de elementos procedimentales a seguir en el ámbito de esta Defensoría del Pueblo de la Ciudad.

La Dirección General de Asuntos Legales, en su carácter de Servicio Jurídico Permanente, ha tomado la intervención de su competencia.

Por ello y en uso de las facultades que le confiere la Ley 3, artículo 13 inc. n) y o)

**EL DEFENSOR DEL PUEBLO
DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES
DISPONE:**

Artículo 1º: REGLAMENTAR el uso de la FIRMA DIGITAL en el ámbito de esta Defensoría, conforme las pautas establecidas en el Anexo I, que a todo efecto forma parte integrante de la presente.

Artículo 2º: FACULTAR a la Autoridad de Aplicación, a la Autoridad de Registro y a la Comisión de Infraestructura Digital en este ámbito estipuladas en el Anexo I de la

presente, en el marco de sus respectivas competencias, al dictado de todo acto y/o instrucción referida al normal desenvolvimiento administrativo del uso de la Firma Digital.

Artículo 3º: ESTABLECER el módulo "COMUNICACIONES OFICIALES" (CCOO), como herramienta de soporte para la creación, comunicación y tramitación de notas, memorandos, y toda otra documentación pertinente de uso interno de esta Defensoría, siendo interfaz de utilización obligatoria y excluyente del soporte papel, sin perjuicio de circunstancias especiales que así lo requieran en contrario. El uso de este módulo será exclusivo y obligatorio por parte del personal jerárquico de la Institución.

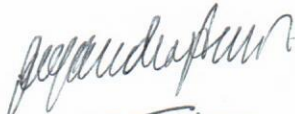
Artículo 4º: Las notas, los memorandos, y toda otra documentación pertinente será remitida a través del módulo CCOO y firmados digitalmente hacia y por el personal jerárquico de esta Defensoría exclusivamente. Estos documentos, se tendrán por comunicados fehacientemente a partir de la confirmación automática de su recepción.

Artículo 5º: El personal jerárquico debe verificar diariamente el módulo CCOO a su cargo con la mayor inmediatez evitando la acumulación de las comunicaciones, siendo responsables de mantener el resguardo y control de su clave de usuario.

Artículo 6º: La presente entrará en vigencia a partir del día de implementación del módulo de Comunicaciones Oficiales, por parte de la Unidad de Modernización y Tecnología, de esta Defensoría.

Artículo 7º: Regístrese, Comuníquese, Archívese.

DISPOSICIÓN Nº 089 / 16


Alejandro Amor
Defensor del Pueblo de la
Ciudad Autónoma de Bs. As.



ANEXO I

Disposición N° 089/16

Uso de Firma Digital

CAPITULO I

Lineamientos Generales

Artículo 1°: Objeto. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente reglamentación.

Artículo 2°: Alcance. La presente regulación comprende el uso de la firma electrónica y de la firma digital por parte del personal autorizado por la Autoridad de Aplicación de esta Defensoría, para el exclusivo cumplimiento de los fines oportunamente encomendados en el marco de su función administrativa.

La utilización de un certificado digital, para finalidad distinta de los fines para los cuales fue extendido respecto del ejercicio de la función administrativa de esta Defensoría; o una vez revocado, generará las responsabilidades correspondientes imputables de manera exclusiva al funcionario interviniente.

El uso de la firma electrónica y digital por fuera de los alcances de la presente, se rige por la normativa de orden nacional y local vigente.

Artículo 3°: Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital es susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permite identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

La firma digital tiene para esta Defensoría y según normativa vigente Ley 2571 para el sector público de la Ciudad Autónoma de Buenos Aires, idéntica eficacia y valor probatorio que sus equivalentes en soporte papel o cualquier otro soporte que se utilice a la fecha de entrada en vigencia de la presente.

1

Artículo 4°: Del requerimiento de firma. Cuando la ley o norma interna de esta Defensoría requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley o norma interna establece la obligación de firmar o prescribe consecuencias para su ausencia.

Los términos del presente no son aplicables a los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.

Artículo 5°: Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

Artículo 6°: Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.

Artículo 7°: Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.

Artículo 8°: Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

Artículo 9°: Validez. Una firma digital es válida si cumple con los siguientes requisitos:

- a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante;
- b) ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente; y



- c) que dicho certificado haya sido emitido o reconocido, según el artículo 26 de la presente, por la Autoridad Certificante ("AC") del Gobierno de la Ciudad, siendo actualmente la Agencia de Sistemas de Información.

Artículo 10: Remitente. Presunción. Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente.

Artículo 11: Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales.

Artículo 12: Conservación. La exigencia de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.

CAPITULO II

De los certificados digitales

Artículo 13: Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por la Autoridad Certificante ("AC"), que vincula los datos de verificación de firma a su titular.

Artículo 14: Requisitos de validez de los certificados digitales. Los certificados digitales, a efectos de garantizar su validez, son emitidos por la "AC", respondiendo a formatos estándares reconocidos internacionalmente, y contienen como mínimo, los datos que permiten:

- a) Identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;
- b) ser susceptible de verificación respecto de su estado de revocación;
- c) diferenciar claramente la información verificada de la no verificada incluidas en el certificado;

- d) contemplar la información necesaria para la verificación de la firma;
- e) identificar la política de certificación bajo la cual fue emitido.

Artículo 15: Período de vigencia del certificado digital. El certificado digital es válido únicamente dentro del período de vigencia que comienza en la fecha de inicio y finaliza en su fecha de vencimiento, siendo ambas indicadas en el certificado digital, o su revocación si fuere revocado. La fecha de vencimiento del certificado digital referida en ningún caso puede ser posterior a la del vencimiento del certificado digital de la "AC".

Del suscriptor

Artículo 16: Suscriptor Certificado. Se entiende por suscriptor de un certificado digital, al funcionario habilitado por la Autoridad de Aplicación, que solicita y obtiene un certificado digital validado por la Autoridad de Registro ("AR") y emitido por la Autoridad Certificante ("AC") prevista en la presente reglamentación.

Artículo 17: Derechos del titular de un certificado digital. El titular de un certificado digital tiene derecho:

- a) A ser informado por la Autoridad Certificante, con carácter previo a la emisión del certificado digital, y utilizando un medio de comunicación sobre las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de este sistema de licenciamiento y los procedimientos asociados. Esa información deberá darse por escrito en un lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;
- b) a que la Autoridad Certificante emplee los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por él, y a ser informado sobre ello;
- c) a utilizar el su certificado digital para el exclusivo cumplimiento de las tareas encomendadas.

Artículo 18: Obligaciones del Suscriptor. Son obligaciones del suscriptor de un certificado digital:

- a) Proveer de modo completo y preciso toda la información necesaria para la emisión del certificado;



- b) mantener el control exclusivo de los datos de creación de firma digital o electrónica, no compartirlos e impedir su divulgación;
- c) informar a la Autoridad de Registro, el cambio de alguno de los datos contenidos en el certificado digital;
- d) solicitar la revocación de su certificado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;
- e) resguardar en todo momento bajo su esfera de custodia el dispositivo criptográfico Token;
- f) utilizar el dispositivo criptográfico para el exclusivo cumplimiento de los fines administrativos para el que le fue encomendado en el ámbito de esta Defensoría.

CAPITULO III

De la Infraestructura Digital

Artículo 19: Conformación. A los efectos del uso de la Firma Digital se establecen los siguientes componentes de la "Infraestructura Digital en la Defensoría del Pueblo de la Ciudad".

- a) Autoridad de Aplicación, conformada por la Secretaría General,
- b) Autoridad de Registro, conformada por la Unidad de Modernización y Tecnología,
- c) Comisión de Infraestructura Digital, conformada de manera no taxativa, por la Secretaría General, por la Dirección General de Asuntos Legales, por la Dirección de Asuntos Legales, por la Unidad de Modernización y Tecnología, por la Unidad de Gestión y Administración Digital, y por la Unidad de Políticas y Programas de Descentralización.

El ejercicio de las funciones de los componentes no supone la percepción de suplemento salarial alguno a tal efecto.

4

De la Autoridad de Aplicación

Artículo 20: Autoridad de Aplicación. La Secretaría General de esta Defensoría es la Autoridad de Aplicación conforme la presente reglamentación.

Artículo 21: Funciones. Son funciones de la Autoridad de Aplicación:

- a) Designar a los funcionarios autorizados para la solicitud y uso de la firma digital en el orden de sus competencias;
- b) solicitar la revocación de uso de los certificados digitales ante la Autoridad de Registro según las causales establecidas en la reglamentación; y
- c) impulsar todo acto y/o instrucción conducente a la implementación de las nuevas tecnologías en la Institución.

De la Autoridad de Registro

Artículo 22: Autoridad de Registro. La Unidad de Modernización y Tecnología de esta Defensoría es la Autoridad de Registro ("AR").

Artículo 23: Funciones. La Autoridad de Registro tiene las siguientes funciones:

- a) Designar los agentes que bajo su responsabilidad y dependencia se desempeñarán como responsables de registro;
- b) recibir, autenticar, validar y autorizar las solicitudes de emisión y/o revocación de certificados digitales y remitirlas a la Autoridad Certificante;
- c) validar en conjunto con la Sub Dirección de RRHH la identidad y cargo de los solicitantes y autenticar los datos de los titulares contenidos en los certificados digitales;
- d) archivar y conservar toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo a los procedimientos establecidos;
- e) corroborar la validez de los datos de los titulares de certificados que se presenten ante ella.
- f) impulsar todo acto y/o instrucción conducente a la implementación de las nuevas tecnologías en la Institución.

De la Comisión de Infraestructura Digital

Artículo 24: Comisión Infraestructura Digital. Tiene como objetivo principal, el desarrollo de las acciones necesarias para la implementación de las nuevas



tecnologías. Posee una integración dinámica que se adecua a sus necesidades operativas.

Sin perjuicio de ello, se forma principalmente por personal de: la Secretaría General, la Dirección General de Asuntos Legales, la Dirección General Económica y Financiera, la Unidad de Modernización y Tecnología, la Dirección de Asuntos Legales, el Consejo de Planificación y Pensamiento Crítico, la Unidad de Gestión y Administración Digital, y la Unidad de Políticas y Programas de Descentralización.

A los efectos de una dinámica fluida de trabajo, la dirección de la Comisión está a cargo de la Unidad de Modernización y Tecnología, quien planifica las líneas de acción y establece prioridades en su tratamiento. A su vez, la coordinación de la Comisión está a cargo de la Unidad de Gestión y Administración Digital, quien bajo la órbita de la Dirección General de Asuntos Legales encauza y articula el trabajo conjunto de los distintos integrantes.

Se reúne periódicamente a los efectos del desarrollo de políticas coordinadas orientadas a la implementación de las nuevas tecnologías en el ámbito de esta Defensoría.

Artículo 25: Funciones. La Comisión emite informes, coordina políticas y realiza las acciones que estima conducentes sobre los siguientes aspectos:

- a) Grado de desarrollo de la aplicación de las nuevas tecnologías;
- b) identificación de las necesidades y acciones conducentes para su plena aplicación;
- c) acciones de capacitación vinculadas a la aplicación de las nuevas tecnologías; y
- d) evaluación de la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como también el cumplimiento de las especificaciones de los procedimientos y los planes de seguridad y de contingencia aprobados.

CAPITULO IV

Del Certificador Licenciado o Autoridad Certificante (CA)

Artículo 26: Del certificador licenciado. El certificador licenciado es la Autoridad Certificante (AC). Es una figura externa a la organización de la Defensoría del Pueblo y se rige por la normativa del ámbito nacional y local.

Dicha Autoridad está en cabeza de la Agencia de Sistemas de Información del Gobierno de la Ciudad (ASI) 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 27: Funciones. A título informativo se deja establecido que según normativa Local, la Autoridad Certificante ("AC") recibe las solicitudes de emisión de certificado digitales, firmada digitalmente con los correspondientes datos de verificación de firma digital del solicitante por la Autoridad de Registro ("AR"), siendo esta última la Unidad de Modernización y Tecnología de esta Defensoría.

Asimismo, la "AC" emite los certificados digitales de acuerdo a lo establecido en sus políticas de certificación, las cuales son aceptadas e informadas por la Autoridad de Registro a los suscriptores para su aceptación.

La "AC" revoca los certificados digitales por él emitidos:

- a) A solicitud del titular del certificado digital;
- b) si determinara que un certificado digital fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación;
- c) si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros;
- d) por condiciones especiales definidas en su política de certificación;
- e) por resolución judicial o de la Autoridad de Aplicación de esta Defensoría del Pueblo.

Artículo 28: Obligaciones. Conforme la normativa vigente, son obligaciones de la "AC" entre otras y al mero efecto enunciativo:

- a) Informar a quien solicita un certificado con carácter previo a su emisión las condiciones precisas de utilización del certificado digital, sus



características y efectos de la revocación de su propio certificado digital. Esta información deberá estar libremente accesible en lenguaje fácilmente comprensible e idioma nacional. La parte pertinente de dicha información también estará disponible para terceros;

- b) mantener el control exclusivo de los datos utilizados para generar su propia firma digital y electrónica e impedir su divulgación y/o acceso a terceros no autorizados;
- c) mantener la confidencialidad de toda información que no figure en el certificado digital y a la que tenga acceso en ejercicio de las funciones definidas en el artículo precedente;
- d) publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales válidos y los revocados, las políticas de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que determine la Autoridad de Aplicación;
- e) revocar los certificados digitales emitidos en caso de verificar que los procedimientos de emisión y/o certificación han dejado de ser seguros;
- f) comunicar a la Autoridad de Registro cualquier irregularidad detectada respecto de la información suministrada por el titular del certificado;
- g) responder por la validez de los certificados digitales emitidos;

CAPITULO V


Revocación del Certificado Digital. Sanciones

Artículo 29: Revocación de certificados digitales. Causales de revocación. Se podrán revocar los certificados digitales emitidos en los siguientes casos:

- a) A solicitud del titular del certificado digital;
- b) si fue emitido sobre la base de una información falsa;
- c) si se determina que los procedimientos de validación y verificación han dejado de ser seguros;

- d) por Resolución de la Autoridad de Aplicación debidamente fundada;
- e) por fallecimiento del titular;
- f) por renuncia al cargo o cumplimiento del mandato;
- g) por declaración judicial de ausencia con presunción de fallecimiento del titular;
- h) por declaración judicial de incapacidad del titular;
- i) si se determina que la información contenida en el certificado ha dejado de ser válida;
- j) por disposición del Defensor del Pueblo.

Artículo 30: Sanciones. Régimen. En el caso de incumplimiento de los deberes impuestos en lo relativo al uso de la Firma Digital y las nuevas tecnologías, la instrucción sumarial y la aplicación de sanciones por violación a disposiciones de la presente se ajusta a lo dispuesto por el Anexo VI del Convenio Colectivo de Trabajo de la esta Defensoría y su normativa concordante.


Alejandro Amor
Defensor del Pueblo de la
Ciudad Autónoma de Bs. As.