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 los procedimientos de uso de la denominada "Firma Electrónica y Digital" en 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 4º 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: un reto 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.

Como antecedente inmediato de ello, este órgano de garantías, ha celebrado un Convenio de Cooperación con el Ministerio de Modernización de la

Ciudad, a los efectos de nutrirse mutuamente de las experiencias previas y generar un camino de dialogo en consonancia, que tienda a la mejor gestión conjunta, favoreciendo directamente a los vecinos de la Ciudad.

A su vez, en el mes de diciembre de 2015, se suscribió un nuevo Convenio Marco de Cooperación y Asistencia Técnica, con la Agencia de Sistemas de Información del Gobierno de la Ciudad (ASI) a los efectos de "*...procurar colaboración para avanzar en el mutuo fortalecimiento institucional en materia de Infraestructura y Servicios Tecnológicos y de Comunicaciones.*"

En su Clausula Segunda se estableció que cada una de las actividades que se determinan, se instrumentan a través del ANEXO I, por medio de los representantes designados. A tal efecto, se estableció que el funcionario responsable de la Unidad de Modernización y Tecnología de esta Defensoría del Pueblo, es el enlace operativo, a los efectos de la planificación, organización, coordinación y ejecución de las actividades de colaboración recíproca a materializarse.

En el Anexo I, se establecieron los lineamientos y requisitos generales para la utilización de la "Infraestructura de Firma Digital (PKI) de la ASI" para la generación de certificados avalados por dicha Autoridad Certificante.[1]

Entre ellos, se contempla la definición por esta Defensoría de una plataforma sobre la que se generarán las claves públicas/ privadas de las solicitudes, debiendo ser aprobada posteriormente por la ASI. Asimismo, se contempla el desarrollo de "Guías y Procedimientos" de solicitud, renovación y revocación de los Certificados para Suscriptores, en un todo conforme con la normativa vigente, cumpliendo específicamente con la "Política de Certificación de la Autoridad Certificante" para las Autoridades de Registro.

No pasa por alto que una de las ventajas fundamentales de la utilización de la "Firma Digital" y de la "Firma Electrónica" radica en brindar mayor celeridad en

1 Conforme Ley 2689, la Agencia de Sistemas de Información (ASI) dependencia Fuera de Nivel, bajo la supervisión de la Jefatura de Gabinete de Ministros, es el órgano rector en materia de tecnologías de la información y las comunicaciones en el ámbito del Poder Ejecutivo GCABA.

los trámites y procedimientos. 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.

En base a ello, el dictado de la presente Disposición resulta necesaria a efectos de aprobar los procedimientos a seguir por el suscriptor de un certificado digital, y la Autoridad de Registro para el empleo de la Firma y Digital, en el ámbito de esta Defensoría del Pueblo de la Ciudad.

Asimismo, en consonancia con los objetivos propuestos, a los efectos de la implementación eficaz de los nuevos sistemas informáticos, se estima razonable convocar por un plazo prudencial a todos los funcionarios jerárquicos de la institución a gestionar a través de la Unidad de Modernización y Tecnología sus respectivos Certificados Digitales.

Consecuentemente resulta imprescindible el desarrollo y puesta en marcha de un plan de capacitación a los efectos de adquirir los conocimientos necesarios respecto de los alcances y responsabilidades que implica el uso de estas nuevas tecnologías por parte de los distintos agentes intervinientes.

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.- RATIFÍCASE a la Unidad de Modernización y Tecnología de esta Defensoría, como enlace operativo frente a las autoridades locales correspondientes, para su constitución como Autoridad de Registro, a fin de gestionar los Certificados Digitales.

Artículo 2º.- DESÍGNASE responsable de la actividad de registro al Ing. Germán Perrone. La asignación de funciones precedentes no implica el pago de adicionales. El responsable de la actividad de registro podrá, por razones operativas, delegar en el agente que él designe las tareas encomendadas, sin que ello signifique deslinde de responsabilidad alguna por lo actuado.

Artículo 3º.- ESTABLÉCESE como responsabilidades primarias de la Autoridad de Registro las de recibir y autorizar las solicitudes de emisión y/o revocación de certificados digitales y remitirlas a la Autoridad Certificante (ASI) previa comprobación y validación de la identidad y autenticación los datos de las personas físicas que soliciten un certificado digital y se presenten previamente a tal efecto ante la Subdirección de Recursos Humanos. Asimismo el archivo, conservación y confidencialidad de los datos personales de toda la documentación respaldatoria que surja del procedimiento de validación de identidad como del certificado digital es responsabilidad de la Autoridad de Registro.

Artículo 4º.- CONVÓCASE a los funcionarios jerárquicos a que dentro del plazo de treinta (30) días de notificada la presente, soliciten y presten colaboración a la Unidad de Modernización y Tecnología en su carácter de Autoridad de Registro a los efectos de la obtención de sus respectivos Certificados Digitales.

Artículo 5º.- ESTABLÉCESE la obligatoriedad de asistencia por parte de los agentes solicitantes de Certificados Digitales a los cursos informativos sobre el uso de Firma Digital, dictado por los sectores pertinentes, de modo previo y como requisito excluyente para su obtención. La obtención de certificados digitales, implica el conocimiento y aceptación de las condiciones de uso de firma digital, que como Anexo I forma parte integrante de la presente.

Artículo 6º.- APRUÉBASE el procedimiento para la solicitud, renovación y revocación de los Certificados para Suscriptores en el ámbito de esta Defensoría, que como Anexo II forma parte integrante de la presente.

Artículo 7º.- APRUÉBASE el uso de la plataforma desarrollada por la Agencia de Sistemas de Información del Gobierno de la Ciudad Autónoma de Buenos Aires a los efectos de la tramitación de los Certificados Digitales.

Artículo 8º: Regístrese, Comuníquese, Archívese.

DISPOSICIÓN Nº 088/16

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

Defensoría del Pueblo
Ciudad Autónoma de Buenos Aires

ANEXO I

Disposición N° 088/16

CONFORMIDAD CONDICIONES DE USO DE FIRMA DIGITAL EN LA DEFENSORÍA DEL PUEBLO DE LA CIUDAD

Ciudad Autónoma de Buenos Aires, de de 20

En la calidad que invoco al suscribir el presente, manifiesto haber recibido la capacitación obligatoria, de manera previa a la obtención de mi certificado digital, a los efectos de su utilización para el desempeño de mis habituales tareas en el ámbito de esta Defensoría del Pueblo de la Ciudad.

Comprendo los alcances del uso de mí certificado digital, el cual verifica la autoría e integridad de los documentos suscriptos, como también comprendo las obligaciones a mi cargo relacionadas a:

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, 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 del certificado digital ante cualquier sospecha de compromiso de clave o circunstancia que pueda comprometer la llave privada del certificado.

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.

Asimismo manifiesto haber leído y tener conocimiento de la Política de Certificación del Gobierno de la Ciudad, de la presente Disposición, de la regulación de uso de Firma en esta Defensoría y los documentos asociados.

Firma:

Aclaración:

Cargo:

RRHH: Autoridad Aplicación:

ANEXO II

Disposición N° 088/16

GUIA DE PROCEDIMIENTOS PARA LA SOLICITUD, RENOVACIÓN Y REVOCACIÓN DE LOS CERTIFICADOS PARA SUSCRIPTORES.

1. PROCEDIMIENTO

1.1 Lineamientos Generales

El presente documento establece los procedimientos a los que se sujetan la aprobación de solicitudes de emisión, renovación y revocación de los certificados digitales emitidos por la PKI del Gobierno de la Ciudad de Buenos Aires, en el ámbito de esta Defensoría del Pueblo de la Ciudad.

1.2 Solicitud de un Certificado

El certificado digital es generado y luego almacenado utilizando hardware criptográfico (Token) diseñado para tal fin. Deben requerirlo y ser utilizado por los agentes que con responsabilidad jerárquica se desempeñen en el organismo, según los términos de uso de la normativa vigente.

1.2.1 Solicitud de un Certificado Digital utilizando Hardware Criptográfico

Para dar curso a una solicitud de un certificado digital utilizando hardware criptográfico, el agente debe realizar los pasos detallados a continuación.

1.2.2 Contacto de un Suscriptor

El suscriptor debe contactarse con la Subdirección de Recursos Humanos, a los efectos de iniciar el proceso de solicitud. La Subdirección le informará el deber de concurrencia -si es que no lo ha hecho- a la capacitación previa estipulada a los efectos de adquirir conocimientos relativos a los alcances, usos y responsabilidades que acarrea el uso de los certificados digitales. Cumplido ello valida los datos relativos al cargo en la institución, entrega un comprobante impreso y comunica a la

Unidad de Modernización y Tecnología quien en su calidad de Autoridad de Registro (AR) de esta Defensoría asigna y comunica al suscriptor un día, horario y lugar para concretar el pedido de solicitud.

1.2.3 Entrega del Token

Validados los datos personales relativos al cargo y comprobada la asistencia del solicitante a la capacitación previa obligatoria, la AR entregará al suscriptor el Token para generar y luego almacenar el certificado digital emitido.

Para poder continuar con el siguiente paso, el Token deberá estar conectado a la terminal desde la cual se vaya a generar la solicitud.

1.2.4 Generar Solicitud

Personal de la Unidad de Modernización y Tecnología asiste al usuario para que instale el certificado de la Autoridad Certificante (AC) en el navegador.

Se genera la solicitud a través de la plataforma habilitada por la Agencia de Sistemas de Información (ASI) en la opción "Generar Solicitud de Certificado Digital con Token".

A continuación se le es solicitado indicar si acepta o no la Política de Certificación, y posteriormente se le indican las instrucciones para instalar el certificado raíz de la AC.

Debe corroborarse que los datos que figuran en el comprobante sean correctos, y en el caso de encontrar algún error debe subsanarse repitiendo el proceso de solicitud.

Al finalizar este paso deben imprimirse dos copias del comprobante emitido como resultado de la solicitud.

1.3 Verificación de Identidad

El solicitante debe presentar ante la AR, la documentación de validación otorgada previamente por la Subdirección de Recursos Humanos. El responsable de AR, verifica los datos y valida la identidad del solicitante y luego de finalizado el proceso

remite copia a la Subdirección de RRHH toda la documentación obrante para su guarda en el legajo personal del suscriptor, resguardando originales a su cargo.

1.3.1 Firma del Comprobante de Solicitud

Corroborados los datos de los comprobantes emitidos se firman las copias tanto por el suscriptor como por el responsable de la AR, asentando de esta forma que:

a) dicha solicitud fue efectivamente realizada por quien dice ser.

b) el suscriptor ha leído y acepta la Política de Certificación del Gobierno de la Ciudad.

c) el suscriptor ha recibido la capacitación previa respecto del uso y responsabilidades que acarrea el empleo del certificado digital.

Toda la documentación relacionada con la solicitud, de emisión, renovación y/ o revocación del certificado digital del suscriptor es resguardada en copia en el legajo personal del funcionario. Los originales quedan bajo la guarda de la AR.

1.3.2 Aprobación de una Solicitud de Certificado Digital

Luego de que el suscriptor haya efectuado la solicitud del certificado digital en conjunto con el responsable de registro, se debe aprobar dicha solicitud para ser remitida a la AC.

1.3.3 Verificación de Datos

El responsable de registro desde la interfaz administrativa debe buscar la solicitud del suscriptor y verificar que coincidan el número de solicitud, nombre y apellido, número y tipo de documento que figuran en el comprobante firmado por el suscriptor.

1.4 Aprobación y Firma de la Solicitud

Si los datos efectivamente coinciden debe aprobarse la solicitud firmándola digitalmente.

1.4.1 Retiro de un Certificado Digital Solicitado

Una vez que el certificado ha sido aprobado por la AC, recibe en el correo electrónico mencionado en la solicitud, la confirmación de la emisión del mismo y la indicación del sitio web al que debe ingresar para su retiro. Si es el caso, se debe colocar el Token y seguir los pasos que se indican en la página web. El retiro del certificado debe realizarse desde la misma PC que se realizó la solicitud.

1.5 Renovación de Certificados

La AR informará por medio de un correo electrónico al suscriptor de un certificado válido, que el mismo se encuentra próximo a vencer. El suscriptor puede solicitar la renovación. Esto será equivalente a generar un nuevo certificado, pero no resulta necesario que el suscriptor valide nuevamente su cargo ante la Subdirección de RRHH, ni identidad ante la AR.

1.6 Revocación de un Certificado Digital

1.6.1 A solicitud del suscriptor del certificado:

El suscriptor de un certificado puede solicitar su revocación si lo considera necesario, para ello debe remitir a la Subdirección de RRHH el formulario de revocación firmado holográficamente, quien dará aviso al AR.

El responsable de registro debe corroborar los datos presentes en el formulario con los de la solicitud original, verificando que la firma coincida.

Posteriormente genera, aprueba y firma digitalmente la solicitud de revocación solicitada y la remite a la CA.

1.6.2 Otros supuestos

Para los casos previstos en el artículo 14 incisos b, c, d, f, g, h, i, j y k del Decreto N° 1.181/GCBA/08, la Subdirección de RRHH recibirá los requerimientos por parte de la Autoridad de Aplicación o la máxima autoridad de la Defensoría del Pueblo.

2. GLOSARIO

Browser: navegador, programa utilizado para visualizar las páginas web.

AC: autoridad certificante (ASI).

Certificado digital: es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto y su clave pública.

Clave pública y privada: es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje. De forma análoga el remitente usa su clave privada para asegurar la integridad e identidad del firmante del documento o mensaje, corroborando la misma con su clave privada.

Criptografía: consiste en cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que sólo puedan ser leídos por las personas a quienes van dirigidos.

CRL: lista de revocación de certificados.

Drivers: programa cuya función es controlar el funcionamiento de un dispositivo de la PC.

Firma digital o Firma electrónica: es un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje.

La diferencia entre ambas firmas radica en que, en el caso del documento firmado digitalmente, si es verificado correctamente, se presume, salvo prueba en contrario, que proviene del suscriptor del certificado digital y que el mismo no fue modificado,

situación ésta que no ocurre en caso de que el documento se encuentre firmado electrónicamente, ya que se invierte la carga probatoria, y de ser desconocida esta firma, corresponde a quien invoca su autenticidad acreditar su validez.

Hardware criptográfico: La funcionalidad de un periférico HSM es la generación de datos seguros (asegurados mediante criptografía de clave pública o PKI) para su acceso a lo largo del tiempo pudiendo aportar adicionalmente seguridad física. Los datos custodiados por un HSM suelen ser las claves privadas usadas en PKI, y en algunas ocasiones también permiten la protección de claves simétricas.

PIN: (Personal Identification Number o Número de Identificación Personal en castellano) es un valor usado para identificarse y poder tener acceso a ciertos sistemas o artefactos,como un teléfono móvil o un cajero automático.

PKI: (Public Key Infraestructure por sus siglas en inglés o Clave Publica de Infraestructura): es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

Una PKI debe proporcionar:

Autenticidad: la firma digital tendrá la misma validez que la manuscrita.

Confidencialidad: de la información transmitida entre las partes.

Integridad: debe asegurarse la capacidad de detectar si un documento firmado ha sido manipulado.

Indubitabilidad: de un documento firmado digitalmente.

AR: autoridad de registro (Unidad de Modernización y Tecnología DPCABA)

RSA: es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye, y otra privada, la cual es guardada en secreto por su propietario.

Token: dispositivo criptográfico que permite la generación del par de claves necesarias para la generación de un certificado digital, y el posterior almacenamiento seguro de dicho certificado.

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