Séptima Conferencia de Directores de Tecnología de Información, TICAL 2017 Gestión de las TICs para la Investigación y la Colaboración, San José, del 3 al 5 de julio de 2017

Proyecto Ypografí. Implementación de la Firma Digital en la Universidad de Buenos Aires

Diego Ormaza De Paul[a,1], Sandra Barrios[a,2], Eloy Fernandez Severini[a,3]

[a] Coordinación General de Tecnologías de la Información y las Comunicaciones, Universidad de Buenos Aires Pte. Uriburu 860, Ciudad Autónoma de Buenos Aires, Argentina

[1] dormaza@rec.uba.ar, [2] sbarrios@rec.uba.ar, [3] eloy.fernandez@rec.uba.ar

Resumen: En pos de modernizar y adaptar la Universidad de Buenos Aires, hacia una administración más eficiente y transparente promoviendo una mayor accesibilidad a la información pública, se implementó un programa general de mejoras de los procesos y de la calidad en la gestión denominado Programa Universidad Abierta.

Uno de los componentes de este programa es la Firma Digital de los documentos emitidos por la Universidad de Buenos Aires, utilizando la Infraestructura de Firma Digital de la República Argentina (Ley N° 25.506 y sus modificatorias).

En ese marco de gobierno electrónico nace el proyecto Ypografí donde la Coordinación General de Tecnologías de la Información y las Comunicaciones (CGTIC) colaboró con la Secretaría General del Rectorado y Consejo Superior para constituirse como Autoridad de Registro (AR), garantizó la infraestructura necesaria y desarrolló un aplicativo para gestionar y firmar documentos digitalmente.

También se desarrolló una solución que permite verificar y validar el documento en papel con su versión electrónica, a través de la incorporación de un código QR que contiene un link de descarga al documento digital.

Para poder efectuar las firmas cada firmante deberá gestionar su certificado digital.

Abordamos en el presente documento los aspectos funcionales y técnicos más relevantes del proyecto, y la problemática que se presentó en la implementación de la solución a nivel organizacional sobre una estructura burocrática propia de entidades universitarias y una cultura fuertemente arraigada a la firma hológrafa.

Palabras Clave: firma digital, gobierno electrónico, QR, certificado digital

Eje temático: Soluciones TIC para la Gestión.

1 Introducción

El proyecto Ypografí nace en Mayo del 2016, y se encuadra, dentro del Programa Universidad Abierta cuyo objetivo general es "desarrollar e implementar la política de gobierno abierto de la Universidad de Buenos Aires mediante herramientas tecnológicas y de análisis que permitan la apertura de la información pública y la participación ciudadana" [1].

El Programa Universidad Abierta es impulsado por la Secretaría General del Rectorado y Consejo Superior de la Universidad de Buenos Aires, a través de la Subsecretaría de Modernización y Relaciones con la Comunidad. El programa cuenta con un componente de Firma Digital cuyo objetivo es facilitar el intercambio de información segura a través de canales digitales.

La legislación argentina define a la Firma Digital como "el 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 debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma". [2]

Para poder cumplir con ese objetivo la Universidad de Buenos Aires debió constituirse como Autoridad de Registro (AR) de Firma Digital[1], teniendo como Autoridad Certificante (AC) a la Oficina Nacional de Tecnologías de Información (ONTI) dependiente de la Subsecretaría de Tecnologías de Gestión de la Secretaríaa de Gabinete de la Jefatura de Ministros de la Nación. La política única de certificación que surge a partir de la ley, otorga a dicha oficina la calidad de Certificador Licenciado[2].

La AR que se incorpora a la estructura de la AC ONTI requiere de un staff integrado por los siguientes roles: un funcionario Responsable de Autoridad de Registro, dos Oficiales de Registros, como mínimo, y un Responsable de Soporte Técnico. Se agregan en el anexo I las funciones a cargo de cada rol. Todos los roles se capacitan en el Ministerio de Modernización de la Nación, respecto a la temática en cuestión, teniendo los Oficiales de Registro que aprobar obligatoriamente un examen que los autoriza a actuar como tales.

La Universidad de Buenos Aires obtuvo su habilitación como Autoridad de Registro de Firma Digital en Diciembre de 2016.

---

[1] Entidad que tiene a cargo las funciones de recepción de las solicitudes de emisión de certificados y validación de la identidad y autenticación de los datos de los titulares de los certificados.

[2] 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. (artículo 17 de la Ley N° 25.506)

La solución inicial propuesta por la Secretaría General incluía la compra de tokens usb para el almacenamiento de los certificados digitales de cada firmante, la utilización del Acrobat Reader DC como herramienta para la firma digital de documentos PDF, y la generación de un File Server con permisos por carpetas para el almacenamiento de los documentos. El File Server permitiría la navegación por carpeta de los documentos digitales, según su estado de tramitación, Borradores, Documentos Definitivos, Para Firma y Firmados.

Se elaboró un cronograma de tareas en forma conjunta con la Secretaria General, se compraron algunos dispositivos criptográficos y se solicitó ante la ONTI certificados digitales personales para el equipo de trabajo de la CGTIC. Se efectuaron las pruebas correspondientes utilizando como aplicativo de firma el Acrobat Reader DC y el Adobe Reader XI y se determinaron las configuraciones necesarias para operar correctamente la firma digital de documentos PDF.

A partir de la propuesta y las pruebas preliminares se evaluaron otras alternativas, de manera de permitir por una parte, la gestión automatizada y más amigable que genere un workflow entre los firmantes, a partir de documentos definitivos, sin la necesidad de mover documentos por carpetas ni asistir a los firmantes para la identificación de los documentos a firmar y por otro lado la consulta que es llevada a cabo por terceros, de los documentos firmados digitalmente por autoridades y funcionarios de la Universidad.

Desarrollaremos a continuación las características funcionales y técnicas del aplicativo Ypografí.

2 La Solución. Características Generales

Ypografí es un aplicativo que permite la gestión de documentos y su firma digital asociada, según la infraestructura de clave pública.

Su nombre en griego significa “firma” y fue diseñado bajo plataforma web.

Es un sistema multidependencia que podrá utilizarse en forma autónoma pero sobre una base de datos centralizada por las distintas unidades administrativas de la Universidad 13 facultades, el Ciclo Básico Común, 4 colegios de enseñanza media, 3 hospitales, la obra social de salud y el Rectorado y Consejo Superior.

El sistema podrá gestionar distintos tipos de documentos: Certificado de Horario Laboral, Certificado de Antigüedad Laboral, Actas de Consejo Superior, Recibo de Haberes, etc..

Cada firmante deberá gestionar ante la Autoridad de Registro (AR) su certificado digital, integrado por una clave pública y otra privada, que se almacenará por software en la pc del firmante o por hardware, a través de un token usb homologado.

En los casos de solicitudes del certificado digital por hardware, el dispositivo de almacenamiento a utilizar debe adaptarse a los requisitos de la política única de certificación de la ONTI, para lo cual se efectuó una evaluación técnica de los dispositivos criptográficos disponibles en el mercado. Se definió que el dispositivo criptográfico que cumple con las especificaciones solicitadas por la ONTI es MS-IDProtect Token USB with Laser PKI 72kb Java Card. El dispositivo seleccionado

cuenta con certificación FIPS140-2 Level 3, cumpliendo con las siguientes especificaciones técnicas:

Interfaz	USB 2.0 tipo A - Plug and Play
Memoria para Certificados	72KB (EEPROM)
Plataformas soportadas	Java Card™ 2.2.2 GlobalPlatform™ 2.1.1
Transmisión de datos	ISO7816 - Protocolos T=1 y T=0
Seguridad Física	Tamper Evident
Carcasa	LED indicador de actividad
Algoritmos Criptográficos Soportados	RSA2048, RSA1024, RSA512, 3-DES, DES, AES128, AES192, AES256, GOST 28147-89, GOST 3411, Elliptic Curves (EC_FP, EC_F2M)
Algoritmos de Hashing	SHA-1 - SHA-256 - SHA-384 - SHA-512
Certificados	x509 v3
Criptografía	Random Number Generator (RNG) - FIPS Approved Generación de algoritmos "On Board"
FIPS	FIPS 140-2 Level 3 (certificado)
Compatibilidad PKI	Microsoft Crypto API (CAPI) Microsoft Crypto API : Next Generation (CNG) PKCS#11 2.20 (2.01, 2.10 y 2.11) PKCS#1, PKCS#7, PKCS#10 PKCS#15 (opcional) PC/SC
Soporte	VPN y SSLVPN
Resistencia al polvo y al agua	Certificación IP68

El firmante deberá utilizar para la firma su clave privada almacenada en su pc o en un token usb. La clave privada a su vez está protegida por una contraseña que sólo el firmante conoce, de manera que, para cada firma deberá informar la misma. A su vez el dispositivo criptográfico, valida la cantidad de intentos fallidos sobre la contraseña de manera que dejará de funcionar al décimo intento.

La clave privada no es exportable, es decir, no podrá copiarse a otro destino. Ante roturas de la pc del firmante o del token usb, el certificado digital deberá revocarse y se gestionará un nuevo certificado.

El sistema consta actualmente de 3 perfiles, con posibilidad de generar nuevos roles a futuro, Administrativo, Firmante y Superusuario.

El perfil **Administrativo** será asignado a aquellas personas que gestionan la documentación en forma previa y posterior a la firma. Serán los encargados de subir al repositorio los documentos definitivos, sólo en formato PDF, a ser firmados. Por cada documento deberán definirse las siguientes características:

- Nombre del Documento

- Tipo de Documento
- Cadena de Firmantes
- Vinculación con el sistema COMDOC[3]: datos para vincular el documento digital al trámite o expediente en el Sistema Integrado de Seguimiento de Expedientes y Documentos (COMDOC). Informado el número CUDAP[4], identificador unívoco de cada trámite, y accediendo a través de un webservice, se mostrará el título del Expediente o Trámite Interno. Esta característica es opcional.
- QR de Seguridad. Esta característica genera un identificador univoco a través de un hash único que permitirá en una etapa final la consulta del documento digital desde un sitio web de la Universidad.

El documento asumirá un estado "Sin Firmas" y se grabará en la base de datos centralizada en formato binario. A su vez se registrará en la base de datos el contenido del PDF.

De esta forma y haciendo uso de un índice del tipo "Gin"[5], se permitirán búsquedas por texto de cualquiera de las palabras contenidas en el PDF. También se permiten búsquedas por filtros predefinidos cómo: nombre del documento, tipo de documento y Número CUDAP.

El perfil **Firmante** es asignado a aquellas personas que tienen poder de firma sobre los documentos y como ya dijimos anteriormente deberán poseer un certificado digital vigente.

Los documentos podrán firmarse en forma individual o masiva, pudiendo el firmante en este caso, seleccionar un conjunto de documentos que se firmarán en forma concurrente cuando el firmante presione el botón "Procesar Firma".

Los documentos podrán previsualizarse a través de la aplicación, de manera que el firmante pueda disponer y navegar el contenido del documento antes de la rúbrica.

El documento firmado asumirá el estado "Firmado No Finalizado" en los casos de firmantes intermedios en la cadena de firmas, quedando disponible para la firma del siguiente rubricante o el estado "Finalizado" con la firma del último firmante.

Solo los documentos en estado "Finalizado" podrán descargarse.

Será necesario instalar en la pc del firmante los siguientes elementos:

i. Java Runtime Environment (JRE): la herramienta de firma necesita de este componente de software para su ejecución.
ii. Middleware IdProtect Monitor: encargado de interactuar con el token usb del firmante (sólo para los firmantes con almacenamiento soportado por hardware)

El Perfil **Superusuario** es asignado a aquellas personas responsables de la administración del sistema. Entre las funciones comprendidas más relevantes podemos mencionar las siguientes:

- Administración de usuarios.

---

[3] El Sistema Integrado de Seguimiento de Trámites y Documentos es utilizado en la Universidad desde 2010. El sistema COMDOC permite gestionar expedientes, trámites internos, notas, oficios judiciales, comunicaciones internas y pedidos de información pública y realizar su seguimiento a través de una hoja de ruta, de manera independiente del lugar físico donde se originen o transfieran los trámites. El software fue cedido a la Universidad por el Ministerio de Economía de la Nación.

[4] Clave Única de Documentación de la Administración Pública

[5] Generalized Inverted Index

- Gestión de los perfiles y privilegios de acceso.
- Administración de los parámetros generales: tipos de documentos, estructura organizacional de dependencias administrativas, asociación de tipos de documentos a las dependencias administrativas.
- Facultad para recuperar un documento que fue eliminado erróneamente y también de eliminar documentos que se encuentren en estado "Finalizado".
- Acceso al log de errores del sistema, a través de la cual se levantan los mensajes de error e información del sistema.

3 Especificaciones Técnicas

Ypografí

El aplicativo Ypografí está integrado por tres componentes: el aplicativo web, que permite la gestión del documento a través del workflow de firmas, la herramienta de firma y el sitio web de descarga de documentos firmados. Detallaremos a continuación algunas especificaciones técnicas de los componentes:

Aplicación Web

Para llevar a cabo la construcción del sistema web la CGTIC decidió utilizar el framework PHP Laravel, el cual es de código abierto y se desarrolló utilizando la versión 5.4 del mismo. El framework se eligió por ser uno de los más utilizados y reconocidos dentro del ámbito PHP, por incluir MVC[6] como patrón de diseño y por su facilidad para integrar paquetes a través de composer. Dentro del desarrollo se utilizó la librería de Bootstrap 3, de manera que la aplicación pueda ser visualizada en cualquier tipo de dispositivo.

Herramienta de firma

Inicialmente en la búsqueda de alternativas de herramientas de firma digital nos contactamos con la Universidad Nacional del Noroeste de la Provincia de Buenos Aires (UNNOBA), ya que esa institución había implementado la firma digital en diversos procesos. Ellos nos cedieron el código fuente de un applet firmador masivo, el cual había sido desarrollado originalmente por el Consorcio SIU[7](Sistema de Información Universitaria). El motivo por el cual se utilizó dicho applet fue la posibilidad que otorga para interactuar con el hardware del lado del cliente. En nuestro caso va a interactuar con el token usb, en el cual se almacena el certificado digital del firmante. Debido a que los applets dejaron de tener soporte en la mayoría de los navegadores (solo soportado actualmente en Internet Explorer), se efectuó una reingeniería para utilizarlo con la tecnología "Java Web Start", otorgando al aplicativo la característica cross-browser.

Aplicación Web de Descarga de Documentos

Para permitir la descarga de los documentos firmados a través de un código de verificación QR se desarrolló un sitio web utilizando el lenguaje .net C#. Este sitio

---

[6] Model View Controler

[7] El SIU es un Consorcio integrado por Universidades Nacionales Públicas Argentinas que desarrolla soluciones informáticas y brinda servicios para el Sistema Universitario Nacional y a distintos organismos de gobierno.

valida que el documento exista y se encuentre finalizado, es decir, con cadena de firmas completa. A su vez se incorporó un captcha de manera que el documento únicamente se descargue sólo si el mismo se completó en forma correcta, evitando que robots utilicen el servicio. La aplicación web de descarga de documentos utiliza la misma base de datos que la aplicación web.

Base de Datos

El sistema de gestión de base de datos utilizado es postgreSQL 9.4. Dicha elección tiene su sustento en la política de utilización de software de gestión de base de datos de la CGTIC (para entornos Windows SQL Server y para entornos Linux postgreSQL) y como consecuencia de la utilización de herramientas de programación de código abierto. Por otra parte, y dado que Ypografí resguarda los documentos digitales en formato binario, ya teníamos experiencia en la utilización del motor postgreSQL para dicho propósito. El Sistema Integrado de Seguimiento de Trámites y Documentos (COMDOC) aloja actualmente 140.000 archivos en ese formato presentando alta disponibilidad y eficiencia en la gestión de las consultas.

En cuanto al diseño de la base de datos el repositorio Ypografí adoptó el modelo de datos relacional, siguiendo algunos lineamientos que plantea el framework Laravel en cuanto a la utilización de claves primaras subrogadas de manera de aprovechar una mayor performance de búsqueda. Adicionalmente y para salvar la debilidad de esta decisión se instrumentaron algunos mecanismos de validación, definiendo claves alternas foráneas que exigen obligatoriedad de llenado y unicidad y algunos otros criterios de buenas prácticas en el diseño.

Webservice ComDoc

Para consultar los datos del sistema COMDOC se desarrolló un webservice. El mismo recibe como parámetros de búsqueda el tipo y número de CUDAP[8]. En caso de existir el trámite pretendido el webservice devolverá el título del Expediente o Trámite Interno y luego estos datos se guardarán en la base de datos de Ypografí. El webservice fue desarrollado en .net lenguaje C# y consulta a través de un linked server la base de datos del Sistema COMDOC. Los datos del Sistema COMDOC se encuentran almacenados en una base de datos postgreSQL.

Seguridad

Para realizar el proceso de autenticación al sistema Ypografí y dado el esquema de Single Sign On ya implementado (WSO2) a partir del año 2016 para las nuevas aplicaciones desarrolladas por la CGTIC utilizamos el protocolo basado en tokens SAML 2.

Asimismo, y dado que el sitio que alojaría los documentos firmados sería accedido desde internet, se configuró en modo https con certificado SSL y se lo ubicó atrás de un web firewall para sumarle protección a su exposición.

Tanto el sistema Ypografí como el sitio que aloja los documentos firmados cuentan con un esquema de backups con periodicidad diaria, semanal y mensual sobre los sitios webs y las bases de datos.

Infraestructura de Servidores

En la actualidad el sistema Ypografí presenta la siguiente infraestructura de servidores para desempeñar de forma óptima sus funciones:

---

[8] Clave Única de Documentación de la Administración Pública

Servidor	CPU	Memoria	Almacenamiento	Sistema Operativo	Servicio
Aplicación Web Laravel y Base Datos	4 x 2,67 Ghz	4 GB	16+48+16 GB HD	Debian 8	Postgres 9.4
Aplicación Web Descargas Documentos	4 x 2,67 Ghz	6 GB	60 GB. Raid 05 (4x 800GB SAS 10k).	Windows Web Server 2008 R2 64bits	Internet Information Server 7.0
WebService ComDoc	4 x 2,67 Ghz	4 GB	40 GB. Raid 06 (12x 600 SAS 10k)	Windows Web Server 2008 R2 64bits	Internet Information Server 7.0

4 El proceso de firma

A partir de la interacción entre la aplicación web y la herramienta de firma el firmante rubricará los documentos digitales. Detallamos a continuación los pasos a cumplir al momento de la firma:

Desde Componente	Acción
Aplicación Web	1) El firmante accede a la pantalla de firmas, en la cual, solo se visualizarán los documentos que se encuentren en ese momento a la espera de su firma. El firmante selecciona los documentos que desea firmar, uno o varios, y luego presiona el botón “Procesar Firmas”. Siempre estará disponible para el firmante la previsualización en línea de los documentos.
	2) El sistema descarga un archivo ejecutable, el cual contiene los parámetros para inicializar la Herramienta de Firma desde la PC del firmante.
	3) El firmante ejecuta el archivo descargado.
Herramienta de Firma	4) Se solicita al firmante que inserte el token (en caso de firmar con un certificado por hardware).
	5) El firmante visualizará todos los certificados disponibles emitidos por AC ONTI y elegirá el certificado que utilizará en la firma actual.
	6) El firmante presiona el botón “Firmar”.
	7) Se solicita al firmante que ingrese la contraseña secreta del certificado digital, para permitir el acceso a la clave

	privada y efectuar la firma del o los documentos seleccionados en la Aplicación Web.
	8) Los documentos PDF se descargan en la PC del firmante.
	9) Los documentos se firman utilizando el certificado digital seleccionado, siempre y cuando se cumplan las siguientes validaciones satisfactoriamente: i. Los únicos certificados digitales válidos son los emitidos por la AC ONTI. ii. Que el certificado se encuentre actualmente vigente. iii. Que el certificado digital no se encuentre revocado al momento de la firma. Para efectuar dicho control descarga la lista de Certificados Revocados (CRL) de la AC ONTI. iv. Por último se efectúa un control cruzado contra el sistema Ypografí, corroborando que el certificado digital con el que se está efectuando la firma, tenga el mismo Cuil que el del usuario logueado en el sistema. Si los controles no son satisfactorios emite un mensaje de error cancelando el proceso de firma actual.
	10) Se suben los archivos PDF firmados digitalmente a la aplicación web y se persisten en forma binaria en la base de datos.
	11) Se informa al firmante que el proceso de firma culminó.
	12) El firmante cierra la herramienta de firma
Aplicación Web	13) El firmante regresa a la aplicación web y refresca la pantalla. Una vez actualizada la pantalla va a mostrarle los documentos PDF pendientes de firma.

A modo de ejemplo y para tener una idea del tiempo requerido por el proceso de firma, la firma de 1.000 documentos demora 23 minutos. Es decir que por cada documento el proceso demanda aproximadamente 1,38 segundos. Este tiempo podrá variar de acuerdo al tamaño del PDF, las especificaciones técnicas de la pc del firmante y de la conectividad de la red.

5 Implementación de la Solución

En una institución burocrática, y con una cultura organizacional con mucho arraigo en el manejo del papel y en la firma hológrafa, una de las problemáticas a superar es reconocer como válido un documento firmado digitalmente. La dificultad se presenta cuando al observarlo en papel el mismo carece de sello y firma manuscrita por una autoridad competente.

Debido a lo expuesto anteriormente se decidió incorporar a través del sistema Ypografí, dos elementos al documento PDF, el primero a modo de referencia, mostrará la imagen de un escudo por cada firma, y el segundo mostrará un código QR, el cual contiene un link a través del que se podrá efectuar la descarga digital del documento en cuestión.

Estos elementos se añaden como estrategia para favorecer la disminución de la incertidumbre, que se genera en el receptor al recibir un documento firmado digitalmente sobre un soporte en papel, dado que la firma digital no se puede visualizar.

Tanto el escudo como el código QR se agregan sólo en la última hoja del documento, tomando el uso y costumbre de la firma hológrafa y teniendo en cuenta que se firma una vez que se avala el contenido del documento. Cada escudo indicará el apellido y nombre del firmante, el nombre de la Universidad y la fecha y hora de la firma, según el huso horario de la República Argentina, como se puede apreciar en la siguiente imagen:

Los escudos se irán insertando, en el margen inferior de la última hoja del documento, de izquierda a derecha hasta un máximo de cuatro, es decir que el escudo de la última firma se visualizará en el extremo del margen inferior derecho. Si hay más de cuatro firmantes sólo se van a mostrar los últimos cuatro escudos.

El código QR se agregará en el extremo del margen inferior izquierdo de la última hoja del documento. El objetivo del código QR es permitir que los receptores del documento puedan descargar el mismo en formato digital. De esta manera podrán constatar que efectivamente el documento está firmado digitalmente. Estos documentos serán accesibles desde internet.

La lectura del código QR sobre el documento en papel se puede hacer a través de un dispositivo móvil o scanner, el mismo contiene un link que redirigirá a un sitio web de la Universidad. En el sitio web, previo a la descarga del documento digital, se deberá completar un Captcha. La descarga se produce siempre y cuando el documento cumpla los siguientes requisitos: exista, no haya sufrido eliminación y se encuentre en estado “Finalizado”, es decir con cadena de firmas cumplida.

De esta forma el receptor podrá comprobar y validar el contenido del documento y las firmas digitales.

A continuación se muestra un ejemplo del contenido del código QR:

QR

https://fddocs.rec.uba.ar/files/**9f8cabe0771054dd4e85**
5de7f69e0fa2806454e74dde56f66a814d227f9f9ade

Donde https://fddocs.rec.uba.ar/files/ referencia al sitio web que vincula al repositorio de documentos firmados digitalmente por la Universidad y

9f8cabe0771054dd4e855de7f69e0fa2806454e74dde56f66a814d227f9f9ade al hash unívoco de identificación del documento.

Por otra parte, tanto para firmar digitalmente como para poder realizar la verificación de la firma digital de un documento, el receptor debe tener instalados el certificado de la Autoridad Certificante Raíz de la República Argentina y el certificado de la Autoridad Certificante de Firma Digital ONTI, ya que los mismos no están incluidos en los sistemas operativos ni en los navegadores.

También se deben efectuar algunas configuraciones sobre el visor de PDF, en nuestro caso el Adobe Reader XI o el Acrobat Reader DC, para que confíe en la firmas de la AC ONTI.

La instalación de los certificados y las configuraciones al visor de PDF se deben efectuar en todos los potenciales receptores de los documentos firmados digitalmente. En principio se definió que el universo UBA es la audiencia prioritaria, es decir, es necesario permitir que todas las computadoras conectadas a la Red UBA puedan visualizar correctamente las firmas.

Para lograr ese objetivo la CGTIC aplicó las siguientes políticas de grupo de Active Directory sobre las computadoras que se encuentran bajo el dominio de Rectorado, automatizando en 1000 equipos:

i. La instalación de los certificados de clave pública Raíz y el de la Autoridad Certificante ONTI.
ii. La configuración del visor de PDF.

Para el resto de las dependencias de la Universidad y la comunidad en general, con el objetivo de favorecer el conocimiento y la divulgación del concepto de Firma Digital y de permitir su correcta visualización desde el visor de PDF, se generaron tres videos de valor comunicativo:

i. Qué es la Firma Digital
ii. Configuración del equipo para visualizar las firmas digitales
iii. Qué contienen los documentos firmados digitalmente en la UBA

Los mismos podrán ser accedidos desde el sitio institucional de la Universidad.

5 Perspectivas a Corto y Mediano Plazo

La solución esta productiva desde Marzo 2017 y la expectativa a corto plazo es la implementación progresiva sobre documentos emitidos por la Secretaria General y la Secretaria de Hacienda y Administración del Rectorado y Consejo Superior de la Universidad. Entre los documentos identificados a ser firmados digitalmente mencionaremos las Actas de sesión del Consejo Superior, las certificaciones laborales de horarios, las certificaciones de antigüedad en el desempeño del cargo y el Recibo de Haberes.

Respecto a la documentación de carácter laboral se está trabajando sobre una interface con el Portal de RRHH, de manera que, a través de la implementación de una ventanilla electrónica, los docentes y no docentes de la Universidad, gestionen las certificaciones correspondientes. Las certificaciones serán firmadas digitalmente por la autoridad competente y remitidas electrónicamente al interesado. Se estima la implementación de este servicio para Mayo 2017.

A mediano plazo se espera avanzar con la implementación en las Unidades Académicas y demás dependencias de la Universidad a partir del requerimiento de las mismas. Hay documentos candidatos a ser incorporados: Constancia de Alumno Regular, Constancia de Materias Aprobadas y el diploma profesional.

A su vez esperamos que la utilización del procedimiento de firma digital en las distintas áreas de la Universidad sea impulsor de esta tecnología, de manera de obtener un efecto contagio multiplicador, que permita avanzar sobre una Universidad más moderna y transparente en sus actos de gobierno.

6 Conclusiones

La firma digital es una herramienta tecnológica que garantiza la autoría, integridad y no repudio de los documentos firmados, otorgando la misma característica que la firma holográfica. Asimismo, facilita el intercambio de información segura a través de los canales digitales.

La Ley 25.506 de la República Argentina establece una infraestructura de Firma Digital y la reconoce dentro del ámbito jurídico.

Considerando que esta tecnología se encuentra abarcada dentro de los objetivos del Programa Universidad Abierta y como Gobierno Digital en el ámbito de la Universidad de Buenos Aires, nos encontramos habilitados por la Autoridad de Certificación ONTI para ejercer las funciones de Autoridad de Registro y contamos con una infraestructura que permite la gestión de documentos firmados.

Consecuentemente con ese objetivo se desarrolló y se encuentra productivo el aplicativo Ypografí para la firma digital de documentos electrónicos y un sitio web que permite a partir de un código QR verificar la validez del documento. La firma digital permitirá ahorros sustanciales en el tiempo de los procesos de firma y del papel consumido, fortaleciendo una gestión más eficiente, transparente y sustentable con el medio ambiente. Durante el proyecto se evaluaron y resolvieron algunas cuestiones, para mitigar la resistencia al cambio, en una institución con alto arraigo cultural en la firma manuscrita.

Suponemos una implementación progresiva, en documentos de distinta significatividad, de manera de obtener procesos de firma testigos que permitirán poner en conocimiento de mandos medios y autoridades los mecanismos de firma digital y sus respectivos beneficios.

Referencias

[] Resolución Consejo Superior UBA 8239/2013 del 18/12/2013
[2] Ley 25.506 FIRMA DIGITAL art.2,
http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm
15/03/2017

Anexo I Composición de roles de la Autoridad de Registro.

Según Política Única de Certificación de la Autoridad Certificante Oficina Nacional de Tecnologías de Información. V2.0 Diciembre 2014

Responsable de Autoridad de Registro
Es la persona que asume ante la Autoridad de Certificación licenciada la responsabilidad de cumplir las exigencias de implementación de la AR. Asimismo, es el responsable de designar a los agentes que actuaran como Oficiales de Registro en dicho organismo y de notificar las modificaciones en los roles mencionados.
Oficial de Registro
Es quien realiza el proceso de identificación de los solicitantes de certificados como paso previo a la emisión de los mismos validando la documentación presentada por estos. También interviene en los casos de requerimientos de revocaciones.

Para ejercer este rol, es requisito que el Oficial de Registro posea un certificado de firma válido emitido por la AC ONTI donde su clave privada esté resguardada en un dispositivo criptográfico que cumpla con el estándar FIPS 140-2 nivel 2 Overall o superior.

Cada AR constituida en la estructura de la AC ONTI licenciada debe tener por lo menos dos Oficiales de Registro.
Responsable de Soporte Técnico de Firma Digital
Es el responsable de instruir y asistir a los solicitantes y suscriptores en la tramitación de los servicios provistos por el Certificador y así como también acerca de las buenas prácticas en la utilización de la tecnología de firma digital. Además es el responsable de su difusión a los usuarios de esa AR y de instruirlos en el manejo de la operatoria de la tecnología de firma digital de las distintas aplicaciones que requieran su uso.