RÍO NEGRO
UNIVERSIDAD NACIONAL

Plan de implementación de Firma Digital en la Universidad Nacional de Río Negro

Tesina de Grado

Licenciatura en Sistemas

Tesista: Tec. Matías Emanuel Sanhueza

Director: Ing. Juan Cruz Martínez Luquez

Codirector: Lic. Mauricio Tassara

Viedma, Río Negro, Argentina

Julio 2018

Agradecimientos

Me siento orgulloso de haber terminado mis estudios de grado, pero debo admitir que muchas personas participaron en este esfuerzo.

En primer lugar, quisiera agradecer a mi director y codirector de tesina que supieron brindarme su tiempo y conocimientos para poder cumplir este tan ansiado objetivo. Al director de carrera de Lic. en Sistemas que supo motivarme para elegir y seguir eligiendo esta carrera. A los profesores, nodocentes, autoridades de la UNRN y otras personas que me apoyaron en este proceso.

En segundo lugar, agradezco al Laboratorio de Informática Aplicada, del cual formé parte durante tres años, siendo mi primera experiencia laboral. Ahí aprendí, fracasé, realicé cursos, asistí a congresos, participé de capacitaciones, y de proyectos de extensión, entre otras actividades. A todos sus integrantes, muchas gracias.

A mis amigos, que no menciono pero que saben que los tengo presente. Les agradezco por cada consejo y ayuda en todo momento, sin ustedes no hubiese logrado sobrevivir al *loco* mundo universitario. A mis hermanos, que también son mis amigos, gracias por acompañarme en todo momento.

Otro muy especial se lo lleva mi familia, quienes me vieron crecer, avanzar, tropezar, levantar y, sin embargo, nunca dejaron de brindarme su cariño y apoyo incondicional. Gracias tío por enseñarme que no todos los hombres son iguales, que no todos los superhéroes llevan capa. A mi abuelita, mi eterna animadora, atenta, entusiasta y siempre interesada en saber lo que estaba haciendo y cómo estaba procediendo, aunque, probablemente, nunca haya comprendido de qué se trataba.

Por último, esta tesina se la dedico de corazón a mi mamá, sin ella nada de esto hubiese sucedido. Me faltan las palabras para describir lo mucho que me has ayudado a concretar mis sueños. Por todas las veces que ocultaste tus lágrimas y miedos para mostrarme una sonrisa. Te amo mamá, gracias por estar siempre para mí.

Resumen

La firma digital revolucionó las diferentes áreas del conocimiento y las actividades humanas, fomentando el surgimiento de nuevas formas de trabajar, aprender, comunicarse y celebrar negocios, al mismo tiempo que contribuyó a borrar fronteras, comprimir el tiempo y acortar las distancias (Bienvenidos a Firma Digital San Juan, s.f.).

Esta tesis se enfoca en idear un plan para la implementación de la Firma Digital en la Universidad Nacional de Río Negro y así adherirse a la Ley Nacional N° 25506. De esta manera, se busca constituir una Autoridad de Registro que dependa directamente de la Oficina Nacional de Tecnologías de Información. Se pretende evaluar tanto el impacto que tendrá el uso de la firma digital en los procesos diarios de la Universidad, como el planteamiento de una transformación progresiva e integral en el modo de trabajo. Se definirá el proceso de solicitud y otorgamiento de certificados digitales a los agentes, los proyectos involucrados, las herramientas que se emplearán para firmar digitalmente y, por último, el resguardo de la documentación una vez firmada. Para finalizar, se plantearán las conclusiones y avances logrados en el transcurso de la tesis.

Palabras claves: Universidad Nacional de Río Negro, firma digital, documento digital, Oficina Nacional de Tecnologías de Información, Ministerio de Modernización, Argentina.

Tabla de contenidos

Tabla de figuras

Capítulo 1: Introducción

A lo largo de los últimos años, la naturaleza de los sistemas informáticos ha ido evolucionando de forma vertiginosa como consecuencia de los grandes avances tecnológicos de la segunda mitad del siglo XX. La sociedad de la información no es un término vacío de contenido o un pronóstico acerca de la influencia de la tecnología en nuestra vida cotidiana. Todo lo contrario, se trata de una nueva revolución sociológica que ha modificado algunos de los hábitos más cotidianos consiguiendo transmitir a la humanidad la sensación de proximidad y la posibilidad de acceder a un número ilimitado de servicios y datos en continua expansión (Reverte, 2002, p.1). Internet es la prueba de ello. Hoy en día, es uno de los medios de comunicación de mayor difusión e impacto, quizá el más directo y dinámico, que ha permitido poner en contacto a personas de todo el mundo a un costo accesible.

Esta constante evolución de la tecnología ha generado que los sistemas hagan mucho más dinámicos los procesos y que las organizaciones puedan interactuar de una manera más fácil utilizando documentación digital. Por otro lado, la exigencia de la *Firma Hológrafa* (firma de puño y letra) para la realización de actos administrativos, unida a los cada vez más crecientes volúmenes de información y documentación en soporte papel, dificultan sin duda los procesos de optimización y modernización de las organizaciones (De Luca, 2005). En efecto, muchos países y regiones están dejando de lado el uso del papel como soporte para realizar sus tramitaciones, tanto en el ámbito local como en el internacional. En su reemplazo, comenzaron a utilizar herramientas más sofisticadas que aseguran una mayor eficiencia en sus procesos y un menor tiempo de respuesta, lo que se traduce en intercambios de información mucho más dinámicos (Pérez, 2009). Sin embargo, uno de los principales desafíos que plantea la utilización de documentos digitales es determinar su autenticidad, es decir la capacidad de asegurar si una persona ha manifestado su conformidad sobre el contenido del documento.

Con la implementación de la *Firma Digital* este desafío quedaría resuelto, ya que ésta es una herramienta que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que gocen de una característica que únicamente era propia de los documentos físicos. Su función respecto de los documentos digitales es similar a la de la firma hológrafa en los documentos impresos, es decir, ser el sello irrefutable que permite atribuir a una persona algo escrito o su conformidad en un documento (Urrego, Vargas Aguirre & Echavarría, 2011).

En Argentina, empresas privadas como Encode (primera empresa privada en certificarse) y entidades estatales como AFIP o ANSES, han implementado con éxito la Firma Digital en diferentes procesos, logrando disminuir gastos de administración, minimizar tiempos de espera e incrementar la confiabilidad de la información transmitida a sus usuarios. La ley de Firma Digital N° 25506, promulgada en el año 2001, habilita el uso del documento electrónico, la firma

electrónica y la firma digital en todo el territorio nacional y, así permite contar con un marco normativo completo en la materia de transacciones electrónicas.

Esta tesis se enfoca en idear un plan para la implementación de la Firma Digital en la Universidad Nacional de Río Negro (UNRN) y así adherirse a la Ley Nacional. Además de esta introducción, los temas se desarrollarán en cinco capítulos más. El segundo está orientado a detallar el contexto del problema que se planea resolver, así como también una posible solución. El tercer capítulo se enfoca en aclarar algunos conceptos y definiciones de Firma Digital, la explicación de su proceso y ciclo de vida. El cuarto capítulo define el marco legal de la firma digital en Argentina, las leyes que la contemplan y las entidades que interactúan en la Infraestructura de Firma Digital de la nación. El quinto capítulo, la solución, describe las tareas a llevar a cabo para constituir a la UNRN como Autoridad de Registro directa de la Oficina Nacional de Tecnologías de Información, las herramientas que se emplean para firmar digitalmente y el resguardo de la documentación una vez firmada. Para finalizar, en el sexto se plantean las conclusiones, futuras recomendaciones y avances transcurridos a lo largo de la tesis.

Cabe destacar que el presente trabajo sólo tiene fines académicos, comprende opiniones y análisis de autores y no compromete en ninguna forma a la Universidad Nacional de Río Negro.

Capítulo 2: Contexto del problema a resolver

2.1 Definición del problema

El continuo crecimiento del consumo de papel, sumado a la necesidad de contar con un espacio físico destinado a su almacenamiento, a la dificultad que implica su traslado, al lento acceso a la información y su tardía actualización son inconvenientes que se presentan en el día a día de la Universidad. Mientras que el uso de la firma hológrafa impide un proceso fluido, la digitalización de los documentos con dicha firma solo sirven para ser archivados. Estos problemas aumentan exponencialmente al contar con sedes físicamente separadas.

2.1.1 Explicación del problema

Río Negro es una de las veintitrés provincias que constituyen la República Argentina. Se encuentra ubicada al centro-norte de la Patagonia y cuenta con una superficie de 203.013 km^2, lo que la convierte en la cuarta provincia más extensa del país.

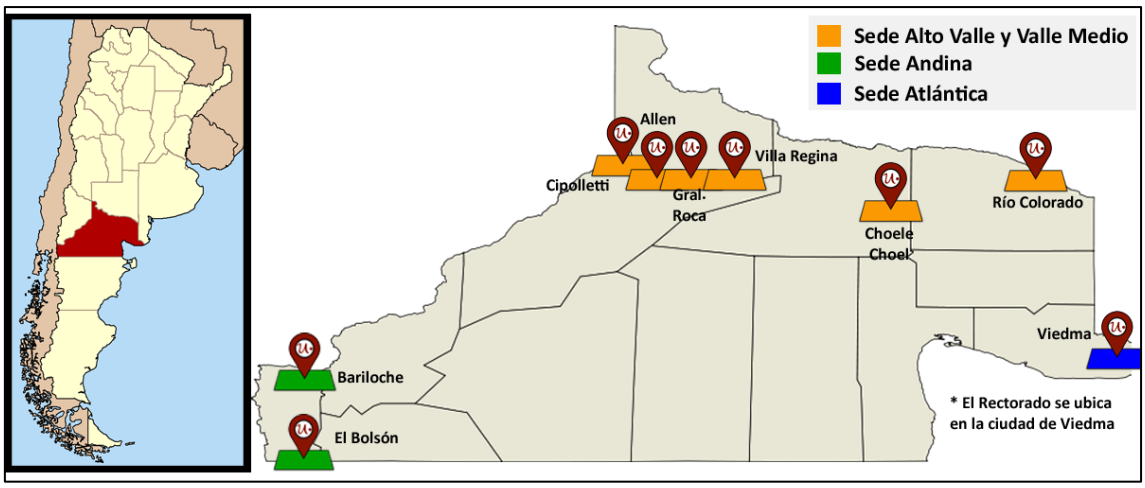


Figura 1: Distribución geográfica de la UNRN

La Universidad Nacional de Río Negro (UNRN), creada en el año 2008 con la vocación de consolidarse como una institución dinámica y emprendedora, se organiza bajo la modalidad de Sedes Universitarias, para dar respuesta a las necesidades de educación, investigación y extensión universitaria de las regiones que conforman el territorio provincial rionegrino. Se basa en los principios de conducción centralizada y operación descentralizada a nivel de cada Sede (UNRN, 2014, Art. 8°). Las Sedes se encuentran ubicadas en distintos puntos estratégicos de la provincia de Río Negro, tales como: Región Atlántica (ATL), Andina (AND) y Alto Valle y Valle Medio (AVVM) (ver Figura 1). Además, también cuenta con dos dependencias en la Ciudad Autónoma de Buenos Aires

(C.A.B.A) y el Rectorado, que se sitúa en la Región Atlántica. En la actualidad, la UNRN alberga, en sus 70 carreras, aproximadamente a mil docentes[1] y a más de diez mil alumnos[2].

Desde su creación, la Universidad acumula alrededor de diecisiete mil seiscientos expedientes en papel repartidos en cada sede[3]. Si bien no son los únicos documentos, algunos pueden llegar a contar con más de quinientas fojas. Es así como la manipulación y almacenamiento que genera el uso de estos archivos en papel implica un gasto significativo en la operatoria diaria de un agente. Si se estima que una persona ocupa tres horas semanales gestionando papel (imprimir, firmar, trasladar, archivar, etc.) (TICPymes, 2015) y la Universidad cuenta con trescientos veintitrés (323) agentes nodocentes[4], que realizan tareas de carácter administrativo, es posible que aproximadamente 900 horas semanales se destinen solamente al papel.

Hoy en día, la firma hológrafa es la forma más utilizada y confiable para relacionar un documento con una persona en particular, de manera legal. Esta firma se emplea para la generación de aperturas de expedientes, resoluciones, disposiciones o notas, entre otras. Sin embargo, al utilizarla entre sedes geográficamente alejadas, ocasiona demoras y deficiencias en los procedimientos que la requieran, ya que es necesaria la presencia física de la persona para realizar dicha actividad. Es decir, si las partes interesadas se encuentran en sedes diferentes, es posible que tengan que hacer el envío del documento en papel, ya sea por servicios de mensajería o transportes de carga terrestre, o tengan que desplazarse hasta un punto de encuentro en común, ocasionando que un procedimiento que debería hacerse en el día se concrete en una semana.

Por otro lado, los documentos firmados hológrafamente que son digitalizados pierden todo valor legal, ya que durante el proceso esa firma, originalmente efectuada de puño y letra, pudo ser editada, alterada, borrada o reemplazada por otra diferente, dando lugar a la desconfianza (De Luca, 2015). En el mundo digital, la particularidad de las tecnologías de información es que utilizan medios electrónicos para realizar intercambios de todo tipo de una computadora a otra, sin necesidad de la utilización de documentos escritos en papel. Sin embargo, la desconfianza anteriormente planteada también se traslada a la sociedad de la información digital, ya que no existe manera de saber quién se encuentra del otro lado de la computadora.

En resumen, la administración de papel, su distribución entre sedes y la desconfianza que generan los documentos digitalizados o producidos sobre

[1] Para más información, ver https://www.unrn.edu.ar/index.php/calidad/estadisticas (01 de marzo de 2017).

[2] Para más información ver https://www.unrn.edu.ar/index.php/la-universidad-nacional-de-rio-negro/historia.(01 de marzo de 2017).

[3] Información provista por el Departamento de Mesa General de Entradas, Salidas y Archivo de la Universidad Nacional de Río Negro el día 12 de diciembre de 2017.

[4] Información suministrada por la Dirección de RRHH de la Universidad Nacional de Río Negro el 14 de diciembre de 2017.

medios electrónicos son las principales causas de la necesidad de contar con una herramienta tecnológica que agregue valor legal al mundo digital.

2.2 Propuesta de Solución

En esta tesis se plantea realizar un plan para llevar a cabo la implementación de la Firma Digital de modo que la Universidad Nacional de Río Negro se adhiera a la Ley Nacional N° 25506. Dicha propuesta tiene como fin disminuir los tiempos de generación y manipulación de un documento para agilizar la operativa diaria de los usuarios, garantizando la autoría e integridad de los mismos a través del uso de la firma digital. Además, dado que no existen barreras geográficas en el mundo digital, sería posible firmar documentos digitales desde múltiples ubicaciones y mediante diversas herramientas de software.

2.2.1 Justificación de la solución

La solución propuesta es pertinente para los siguientes aspectos del problema planteado. En primer lugar, y desde el punto de vista económico, la forma de gestión actual de los documentos dentro de la Universidad tiene un costo elevado. Tanto los trámites como las actividades son registrados en documentos como resoluciones, disposiciones, informes, notas, órdenes administrativas, recibos de haberes, entre otros. Un alto porcentaje de estos documentos tiene como soporte físico el papel, con el agravante de que, a veces, se exigen copias adicionales para distribuirlas a diferentes dependencias o autoridades que las requieren. Además, como paso previo a la versión final, frecuentemente se imprimen hasta dos o tres borradores para revisión y generalmente solo se utiliza una cara de la hoja. Una consecuencia adicional de este mismo hecho es la necesidad de adquirir materiales de impresión e incluso inmuebles destinados al almacenamiento de documentación física. Por ejemplo, en diciembre de 2017, la Secretaría de Investigación, Creación Artística, Desarrollo y Transferencia de Tecnología (SICADyTT) utilizó veinte (20) resmas de papel a un valor de $ 130 por resma[5]. Si se parte de que un árbol equivale a dieciséis (16) resmas[6], la SICADyTT dejó fuera del ecosistema natural a 1.25 árboles, es decir que durante el año 2017 empleó alrededor de 192 mil hojas, a un coste monetario de $ 31200 pesos y un coste natural de 15 árboles, aproximadamente.

En segundo lugar, desde el punto de vista del rendimiento, la firma digital, unida a la obligatoriedad de utilización de documentos electrónicos, incrementa la eficiencia de los procesos de trabajo permitiendo ahorrar tiempo (Mesa Sánchez, 2015). La utilización del papel como soporte de información en trámites y procedimientos exige disponer de espacio físico para su archivo, pesa demasiado, y resulta ineficaz su procesamiento, requiriendo de la acción

[5] Según registros presupuestarios provistos por Unidad de Vinculación Tecnológica de la UNRN el día 19 de marzo de 2018.
[6] Para más información ver http://conservatree.org/learn/EnviroIssues/TreeStats.shtml.

humana, ya sea al archivar, recuperar o compartir información. La tecnología nos permite transferir la información en papel a soportes digitales, agilizando su envío y recepción. Es decir, los procesos y los flujos de operaciones que implican la firma y gestión de documentos se automatizan, simplificando en gran medida no sólo el procedimiento en sí, sino la gestión del papel en general.

Por último, desde el punto de vista de la seguridad de la información, la firma digital brinda garantía de autoría e integridad de los documentos digitales, pero no confidencialidad ya que un documento firmado digitalmente puede ser visualizado por otras personas, al igual que cuando se firma hológrafamente (Pérez Jurado, 2009).

Al utilizar la firma hológrafa, ésta es tan identificable como una huella digital, de alguna manera. Pero, como una huella digital, el autógrafo es solo una marca unidimensional en papel, y no especifica mucho sobre lo que sucedió realmente cuando se firmó un documento. Una firma digital, por otro lado, es como una huella digital tridimensional. Es decir, que contiene capas de información sobre qué, cuándo, dónde, cómo y quién firmó, creando un rastro robusto de datos que detalla realmente el significado de esa firma (Bates, 2014).

A medida que se avance en la lectura de esta tesis se podrá ver que las firmas digitales en realidad pueden ser más seguras que sus contrapartes hológrafas, más rápidas y menos costosas.

2.3 Objetivo general

Por lo tanto, como objetivo principal se plantea crear un lineamiento que sirva de apoyo para la constitución de la Universidad Nacional de Río Negro como Autoridad de Registro de la Oficina Nacional de Tecnologías de la Información, dentro del marco de Infraestructura de Clave Pública de la República Argentina, según la Ley de Firma Digital N° 25506.

2.4 Objetivos específicos

A continuación, se detallan una serie de objetivos específicos que permiten en conjunto establecer los pasos a seguir para cumplir con el objetivo general:

- Definir los conceptos de firma digital y certificado digital.
- Explicar el marco teórico-legal de la firma digital en Argentina y el Mercosur.
- Determinar los pasos para constituir una Autoridad de Registro, teniendo en cuenta los documentos provistos por la Oficina Nacional de Tecnologías de la Información. Dichos documentos se detallan en el Capítulo 5.

- Evaluar diferentes softwares cliente para el uso por parte de los usuarios finales de la firma digital.
- Proponer un esquema de almacenamiento y resguardo de la documentación firmada digitalmente.

Capítulo 3: Fundamentos de la Firma Digital

En este capítulo se explican los fundamentos y las bases para la implementación y uso de las firmas digitales. Para ello, inicialmente se definen los conceptos de Seguridad de la Información, criptografía y criptoanálisis hasta llegar a la era de la firma digital, pasando por una breve descripción de los algoritmos que impactaron en el mundo de la criptología.

Posteriormente, se explicará la infraestructura que soporta el uso de la criptografía de clave pública y las firmas digitales como formatos que definen la estructura e información, hasta finalizar con los aspectos relacionados con la certificación de la identidad desde el punto de vista del formato de sus certificados y la gestión de su ciclo de vida.

3.1 Seguridad de la Información

Antes de hablar de firma digital, hay que tener en cuenta qué es la seguridad de la información ya que todo sistema que procese, almacene o transmita información tiene que cumplir con una serie de requisitos. En primer lugar, ha de preservar la información frente a alteraciones tanto fortuitas como deliberadas, debidas a fallos en el software o en el hardware, provocadas por agentes externos (incendios, interrupciones en el suministro eléctrico, etc.) o por los propios usuarios. En segundo lugar, debe evitar accesos no autorizados tanto al sistema como a su contenido. Finalmente, el sistema debe garantizar que la información esté disponible cuando sea necesario. Estos tres requerimientos quedan recogidos en los conceptos de *integridad*, *confidencialidad* y *disponibilidad* de la información respectivamente, y son los que hacen que se pueda considerar seguro a un sistema.

En otras palabras, la seguridad de la información se define como el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener no solo los tres requerimientos mencionados anteriormente, sino también la autenticidad y el no repudio de la misma.

- La autenticidad es el mecanismo que permite conocer si la persona que está accediendo al sistema es realmente quien debe acceder y no un extraño.
- La confidencialidad hace referencia a la imposibilidad de acceder a información protegida por parte de todas aquellas entidades que no han sido autorizadas para tal efecto.
- La integridad proporciona los mecanismos necesarios para detectar cualquier posible modificación o eliminación llevada a cabo por parte de alguna entidad no autorizada.

- El término disponibilidad hace referencia al grado en el que un sistema o componente está operativo y accesible cuando es necesario hacer uso de este.
- El no repudio es la garantía de que tanto el emisor como el receptor de un mensaje poseen las evidencias necesarias como para que ninguno de ellos pueda negar su participación en la comunicación. (Reverte, 2002, p.3).

La protección de la información se basa en el hecho de poder diferenciar entre las entidades que han sido autorizadas y las que no. Por lo tanto, garantizar la seguridad de un sistema informático es un objetivo mucho más amplio y complejo que la simple protección de los datos mediante técnicas criptográficas. De hecho, se debe tener en cuenta múltiples factores, tanto internos como externos. (Lucena López, 2010, p.39)

3.2 Criptografía y Criptoanálisis: bases de una seguridad robusta

La palabra criptografía proviene del griego *kryptos*, que significa esconder y *graphein*, que significa escribir, es decir, escritura escondida. Entonces, el emisor aplica técnicas criptográficas para poder "esconder" el contenido del mensaje (de ahora en más lo llamaremos cifrar o encriptar) y lo envía por un canal de comunicación que se supone inseguro. Sólo el receptor autorizado puede leer el contenido "escondido" del mensaje (lo llamaremos descifrar o desencriptar) (Molina, 2006). De esta manera, la criptografía es una rama de las matemáticas que hace uso de métodos y técnicas con el objeto principal de cifrar y/o proteger un mensaje o archivo mediante algoritmos, usando una o más claves, de modo que es realmente difícil obtener el archivo original sin poseerlas (Varela Velasco, 2006).

Cabe destacar que la palabra criptografía sólo hace referencia al uso de códigos, por lo que no engloba a las técnicas que se usan para romper dichos códigos, conocidas en su conjunto como Criptoanálisis. El criptoanálisis (del griego *kryptos*, "escondido" y *analýein*, "desatar") es una ciencia que estudia y analiza los sistemas criptográficos con el objetivo de encontrar debilidades y romper su seguridad, sin poseer autorización para hacerlo. En cualquier caso, ambas disciplinas están íntimamente ligadas; no olvidemos que cuando se diseña un sistema para cifrar información, hay que tener muy presente su posible criptoanálisis, ya que en caso contrario podríamos llevarnos desagradables sorpresas (Lucena López, 2010, p.31).

Con el propósito de ocultar información confidencial de los ojos no autorizados y asegurar la detección inmediata de cualquier alteración de esta, los algoritmos criptográficos pueden clasificarse en simétricos o asimétricos. En el primer caso la clave de cifrado y descifrado son iguales, es decir, el emisor cifra un mensaje con la clave privada y el receptor lee el mensaje descifrándolo con la misma

clave. La criptografía asimétrica, en cambio, utiliza un par de claves que están matemáticamente relacionadas pero que son diferentes entre sí. De este modo, se deben crear dos tipos de claves, una pública, que será conocida por todos los receptores del documento digital, y otra privada, que deberá ser mantenida en secreto por el firmante. Ambas son únicas y su creación se produce en forma simultánea.

3.2.1 Criptografía Simétrica o de Clave Privada

La criptografía simétrica es el conjunto de métodos que permite una comunicación segura entre dos partes, siempre y cuando previamente hayan intercambiado una clave secreta llamada clave simétrica. La simetría se refiere a que ambas partes utilizarán la misma llave tanto para cifrar, como para descifrar (ver Figura 2) (Litwak & Escalante, 2004, p.42). Es por ello, que la robustez del algoritmo dependerá directamente de mantener en secreto esa clave.

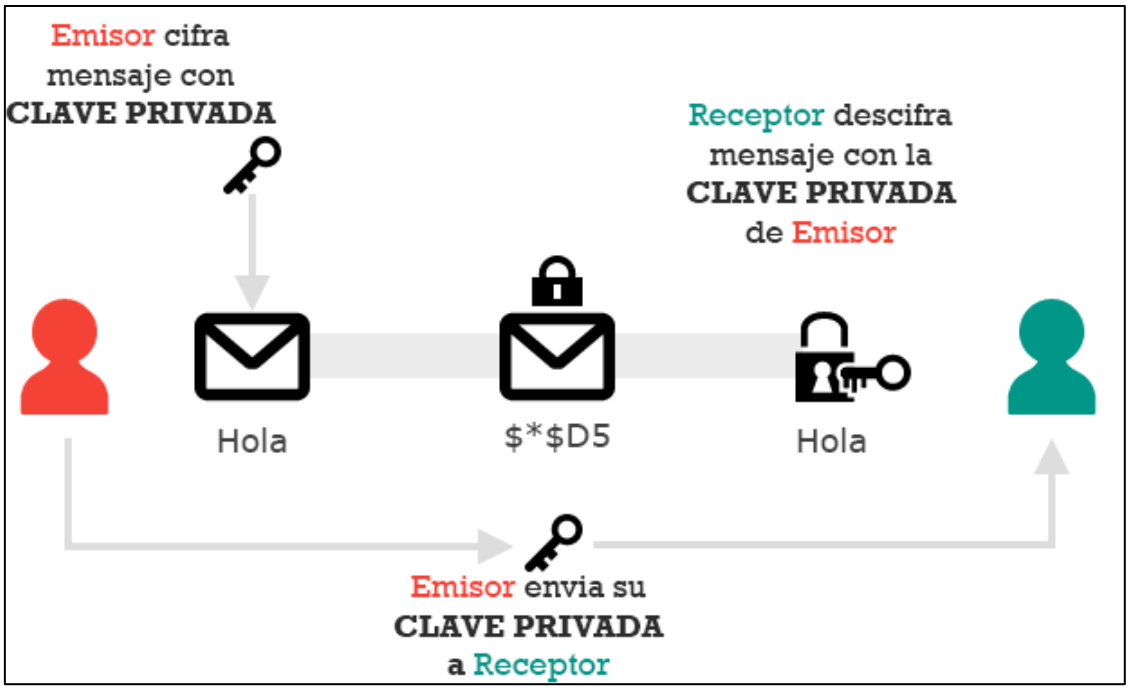


Figura 2: Criptografía Simétrica (Amieva, 2015)

La criptografía simétrica ha sido la más utilizada a lo largo de la historia ya que por su rapidez y facilidad de implementación en distintos dispositivos manuales, mecánicos, eléctricos, así como también en algoritmos programables, resulta apropiada para el cifrado de grandes volúmenes de datos. Sin embargo, las dos claves generadas son idénticas y tanto el emisor como el receptor tienen que conocerlas para establecer una comunicación segura, por lo que la principal desventaja recae en conseguir que ambos lleguen a un acuerdo sobre qué clave

secreta elegir y cómo compartirla en un canal de comunicación que se supone inseguro.

3.2.1.1 Algoritmo DES

Si bien existen muchos algoritmos de criptografía simétrica, DES (Data Encryption Standard, por sus siglas en inglés) es el más estudiado y utilizado mundialmente.

DES es un algoritmo desarrollado originalmente por IBM bajo el nombre de Lucifer. Fue requerido por el NIST (National Institute of Standards and Technology, Instituto Nacional de Estandarización y Tecnología)[7] y posteriormente modificado y adoptado por el gobierno de EE.UU. en 1977 como estándar de cifrado de todas las informaciones sensibles no clasificadas. Posteriormente, en 1980, el NIST estandarizó los diferentes modos de operación del algoritmo. (Litwak & Escalante, 2004, p.54).

Sin embargo, en 1998, la empresa Electronic Frontier Foundation (EFF), con una inversión de un poco menos de 250 mil dólares, ideó una máquina que, mediante la aplicación de un ataque de fuerza bruta, el cual consiste en recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso, descifraba mensajes DES en menos de 3 días (EFF, 1998). Pero la debilidad no recae en el algoritmo en sí, sino en la clave, cuya longitud es finita y demasiado corta (128 bits).

En la actualidad, el algoritmo se considera poco robusto pero su investigación continúa siendo interesante ya que puede ser implementado fácilmente tanto en software como en hardware.

3.2.2 Criptografía Asimétrica o de Clave Pública

Con el fin de resolver el problema de la distribución de claves, Whitfield Diffie y Martin Hellman introdujeron el concepto de criptografía de clave pública en 1976 al presentar un artículo titulado New Directions in Cryptography (Diffie, W. & Hellman, M. E., 1976). La criptografía asimétrica utiliza algoritmos matemáticos relacionados con números primos. Los números primos son aquellos números enteros que son divisibles por sí mismos y por uno. Es por ello qué se consideran como ladrillos que construyen a todos los demás números, ya que cualquier número entero puede descomponerse de manera única como el producto de números primos. Si bien son infinitos, a medida que se avanza en la lista de estos números, se puede observar que cada vez aparecen con menos frecuencia. La manera en la que se distribuyen los números primos dentro de los naturales es de tremenda importancia, no solo para los matemáticos, sino para todo el mundo, o al menos para cualquier persona que utilice Internet (De León, M. & Timón, A., 2014).

[7] Anteriormente NBS (National Bureau of Standards, Oficina Nacional de Estandarización) de EE. UU.

En la criptografía de clave pública, cada usuario del sistema dispone de un par de claves único y, a diferencia de lo que sucedía con la criptografía simétrica, la clave privada no es un secreto compartido, sino que debe ser protegida por cada usuario. Sin embargo, la clave pública debe difundirse con el fin de que otras entidades puedan emplearla para proteger las comunicaciones realizadas con el usuario en cuestión. Este tipo de criptografía, se basa en el hecho de que resulta computacionalmente intratable intentar descubrir una clave a partir del conocimiento de la otra, lo cual anula la necesidad de establecer secretos compartidos entre entidades ya que basta con tener acceso a las claves públicas (Reverte, 2002, p.6). Es decir, la razón por la cual resulta improbable hallar una de las claves en la criptografía asimétrica es porque este sistema está basado en funciones trampa. Una función trampa es aquélla cuyo cálculo directo es sencillo de resolver, mientras que invertir la función implica desarrollar un gran número de operaciones. Por ejemplo, es fácil multiplicar dos números primos juntos para sacar uno compuesto, pero es difícil factorizar uno compuesto en sus componentes primos Dado que la función trampa se basa en la multiplicación de números primos, sería necesario conocer todos los números primos grandes para ser capaz de deducir una clave a partir de otra, pero está demostrado que en la práctica se tardarían demasiados años sólo en el proceso de obtención de los número primos grandes (por ejemplo, números primos de más de 100 cifras).

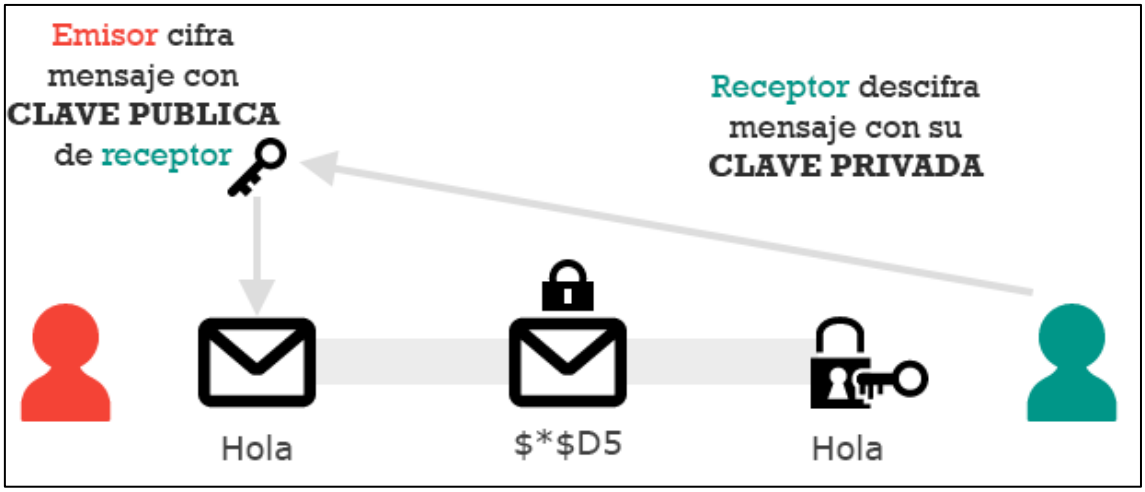


Figura 3: Criptografía Asimétrica (Amieva, 2015)

Para enviar un mensaje confidencial sólo hace falta conocer la clave pública del destinatario y cifrar un mensaje utilizando dicha clave. En este caso los algoritmos asimétricos garantizan que el mensaje original sólo puede volver a recuperarse utilizando la clave privada del destinatario (ver Figura 3). Dado que la clave privada se mantiene en secreto, sólo el destinatario podrá descifrar el mensaje.

Si bien la criptografía asimétrica es más segura que la simétrica, la longitud de sus claves (por lo general cinco o más veces mayores a la clave de la criptografía

simétrica) ocasiona que el mensaje cifrado sea de mayor tamaño y, por ende, necesita mayor tiempo de procesamiento, convirtiéndose en su mayor inconveniente.

Como mencionamos anteriormente, los algoritmos asimétricos proporcionan una mayor seguridad que los simétricos, desde el punto de vista de la confiabilidad, a costa de una mayor carga computacional. Es por esta razón, que, generalmente, se emplea una combinación de ambos denominada *Criptografía Híbrida*.

3.2.2.1 Algoritmo RSA

Este algoritmo, el primero y más utilizado de la criptografía asimétrica, fue inventado por R. Rivest, A. Shamir y L. Adleman (de sus iniciales proviene el nombre del algoritmo) en el Massachusetts Institute of Technology (MIT).

La robustez del algoritmo se basa en la facilidad para encontrar dos números primos grandes frente a la enorme dificultad que presenta la factorización de su producto. Aunque el avance tecnológico hace que cada vez sea más rápido un posible ataque por fuerza bruta, el simple hecho de aumentar la longitud de las claves empleadas supone un incremento en la seguridad del algoritmo. Sin embargo, existe un límite a dicha longitud (Litwak & Escalante, 2004, p.59). Se cree que RSA será seguro mientras no se conozcan formas rápidas de descomponer un número grande en producto de primos.

3.2.3- Funciones Hash o de resumen

Las funciones *hashing* (o hash) juegan un rol fundamental en la Criptografía pues sirven esencialmente para verificar la integridad de los mensajes. Parten de una información de entrada de longitud indeterminada y obtienen como salida un código, que en cierto modo se puede considerar único para cada entrada. Dicho de otro modo, se puede definir que una función hash “comprime” el mensaje, a fines de producir una especie de “resumen” (usualmente de 128 o 254 bits), el cual será comprobado para asegurar que se mantenga la integridad del mismo (ver Figura 4).

La función de estos algoritmos es determinista, es decir que partiendo de una misma entrada siempre se obtiene la misma salida. Sin embargo, el interés de estos algoritmos reside en que partiendo de entradas distintas se obtienen salidas distintas.

Dado que el tamaño del código que se genera como salida es de tamaño limitado, (típicamente 128, 256 ó 512 bits) mientras que el tamaño del documento de entrada es ilimitado (típicamente un archivo), es evidente que se cumplen dos propiedades:

1. El algoritmo es irreversible, es decir, no es posible obtener el documento original a partir del código generado.
2. Existen varios documentos que dan lugar a un mismo código.

La segunda propiedad es debida a que el número de combinaciones de los códigos de tamaño limitado es menor al número de combinaciones de cualquier archivo grande. Es decir que, obviamente, si hay otros mensajes que produzcan el mismo hash es extremadamente difícil encontrarlos y aún más difícil que tengan el mismo contenido o incluso un significado en nuestra lengua. Sin embargo, los buenos algoritmos consiguen que los documentos que dan lugar al mismo código sean completamente diferentes y por lo tanto sólo uno de ellos será legible (Luna, 2012).

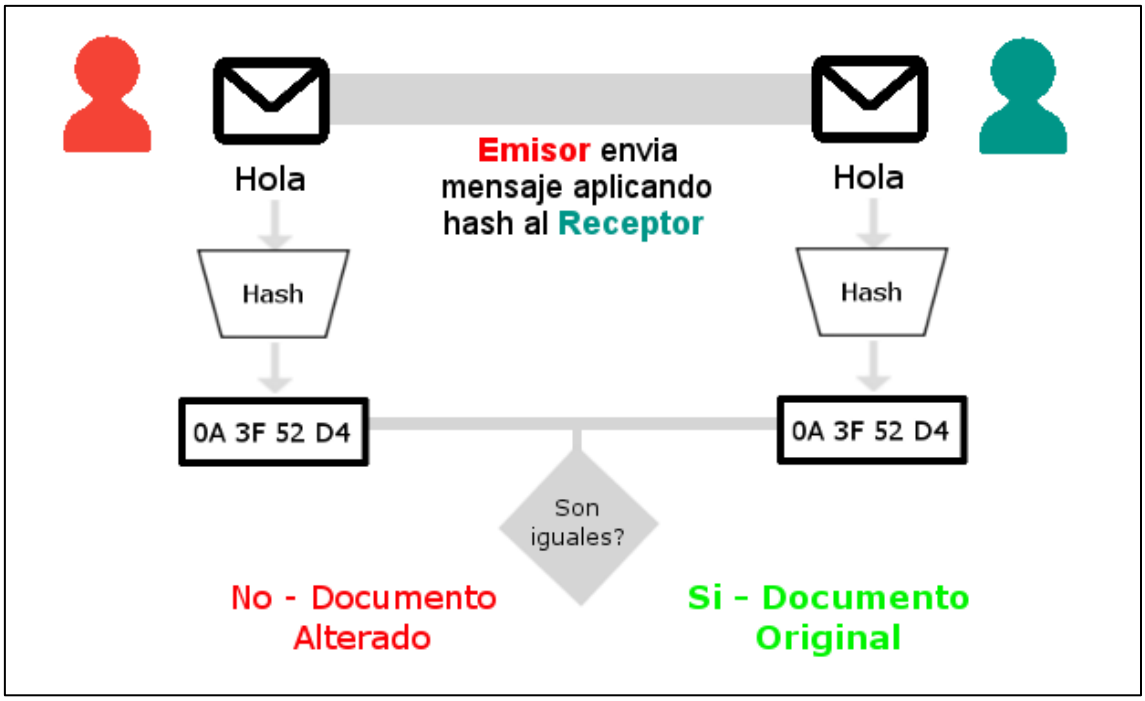


Figura 4: Función Hash

Entre los algoritmos más utilizados se pueden encontrar MD5 y SHA1. MD5, a pesar de haber sido considerado criptográficamente seguro en un principio, Xiaoyun Wang y Hongbo Yu, ambos de la Universidad de Shandong de China, publicaron un artículo en marzo de 2005 en el que describen un algoritmo que puede encontrar dos secuencias diferentes de 128 bytes con el mismo hash MD5. Este proceso que ocurre cuando dos valores de entrada diferentes generan el mismo resumen se denomina colisión hash o ataque por colisión (Wang & Yu, 2005).

Por otro lado, SHA1 (abreviatura de Secure Hash Algorithm 1), el sucesor del MD5, cayó ante Google bajo un proyecto que costó alrededor de 110 mil dólares. Dicho proyecto, denominado SHAttered (un juego de palabras que significa “destrozado” o “hecho pedazos”), también utilizó ataques de colisión para hacer visible la vulnerabilidad de SHA1.

Por estas razones, en la actualidad MD5 y SHA-1 se consideran poco seguros, sin embargo, todavía son utilizados en el ambiente de la programación.

3.3 Firma Digital

En la práctica los algoritmos de clave pública, debido a que requieren mucho tiempo para cifrar documentos largos, se implementan junto con funciones hash unidireccionales dando lugar a lo que llamamos firma digital. De esta manera en vez de firmar un documento, se firma un resumen del mismo.

Entonces, una definición acertada es: “*La firma digital es un proceso matemático, denominado hash, que relaciona el documento digital con información propia del firmante. La clave privada certificada es utilizada por el emisor para cifrar el hash. El valor del hash es exclusivo y cualquier cambio en los datos da como resultado un valor diferente. Este atributo permite a otros validar la integridad de los datos utilizando la clave pública del firmante para descifrar el hash*”.

Por otro lado, podemos decir que la firma digital es una herramienta que dota de ciertos atributos o propiedades a un documento:

- Autenticidad: garantiza la identidad del firmante del documento, es decir, que el documento ha sido firmado por la persona que dice haberlo firmado.
- Integridad: asegura la integridad del mensaje, esto es, que la información contenida en el documento digital no ha sido modificada luego de su firma.
- No repudio: garantiza que el firmante no pueda negar el contenido del documento o la veracidad de la firma. En otras palabras, si un documento es firmado con la llave privada de un individuo, aunque éste no lo haya hecho, debe de reconocer el documento como auténtico. Por lo tanto, debe responsabilizarse por mantener su llave privada en total secreto.

3.3.1 Funcionamiento de la Firma Digital

Como se mencionó anteriormente, el hash relaciona un fragmento del documento digital con información propia del Emisor de dicho documento. Posteriormente, el hash se cifra con la clave privada del Emisor con el objetivo de obtener la firma digital, la cual se agrega al documento en cuestión. El hash es específico a este documento en particular y el mínimo cambio resultará en un hash diferente. Con esto, el Receptor se asegura de que ese documento no ha

sido modificado desde que el emisor lo firmó, obteniendo así, el principio de integridad.

Por otro lado, cuando el Receptor recibe la información, descifra la firma digital con la clave pública del Emisor y obtiene el hash original del documento que envió el Emisor. Luego se calcula el nuevo hash para el documento digital y si es igual al hash descifrado por la clave pública, se dice que la firma digital es auténtica y que el documento no fue alterado. Este proceso es conocido como Verificación de la Firma Digital (ver Figura 5).

Lo que resulta interesante del uso de muchos de los sistemas basados en la criptografía asimétrica es que las operaciones realizadas con una de las claves pueden revertirse empleando la otra. Por ejemplo, en el caso de que cierta información sea cifrada utilizando la clave pública de un usuario, ésta podrá ser descifrada empleado la clave privada. Dado que sólo el usuario tiene acceso a dicha clave, obtenemos de esta forma un medio para proteger la *confidencialidad* de la información. Por otra parte, el cifrado realizado mediante la clave privada también puede deshacerse empleando la clave pública. Aunque esta operación carece de interés desde el punto de vista de la confiabilidad, dado que la clave de descifrado es pública, y por lo tanto conocida por todos, representa un mecanismo muy robusto de *autenticación*. La razón es que sólo hay un usuario capaz de cifrar información que podrá ser descifrada posteriormente con el uso de funciones hash, conocido como mecanismo de firma digital, ya que además de autenticación es capaz de proporcionar servicios básicos de integridad y de no repudio (Reverte, 2002, p.6).

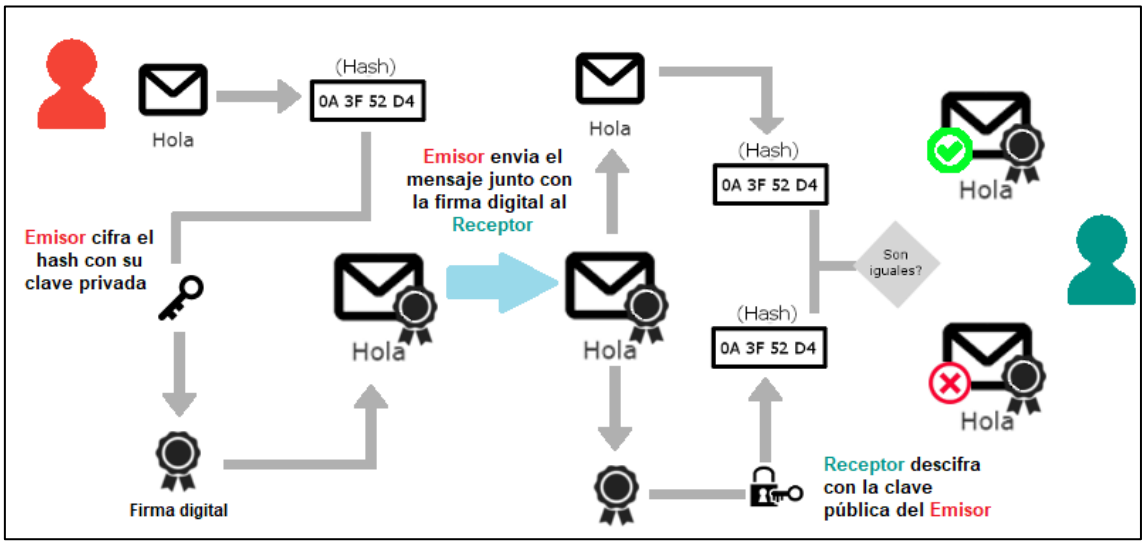


Figura 5: Funcionamiento y verificación de la Firma digital

3.3.2 Diferencias con la firma electrónica y firma digitalizada

Dentro de un marco legal, la firma electrónica es el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a un documento

digital, utilizado por el firmante como su medio de identificación. Este concepto es más genérico, amplio e indefinido desde el punto de vista electrónico que la firma digital.

Sin embargo, la diferencia entre la firma digital y la firma electrónica radica en su valor probatorio. Concretamente, en el caso de la firma digital, si un documento firmado digitalmente es automáticamente verificado como correcto, se presume, salvo prueba en contrario por parte del demandante, que proviene del suscriptor asociado y que no fue modificado. Es decir, adquiere características de documento público, a pesar de ser privado. Esto se conoce como no repudio. Por el contrario, en el caso de la Firma Electrónica, se invierte la carga probatoria con respecto a la anterior. O sea que, en caso de ser desconocida la firma, corresponde a quien invoca su autenticidad acreditar su validez. Por ejemplo, si entre dos partes que celebran un contrato firmado digitalmente (no electrónicamente) y una de ellas alegase la invalidez de alguna de las dos firmas, le corresponde a ésta demostrar ante la ley la invalidez de la misma. En caso de no tener la capacidad de demostrarlo, para la ley argentina esa firma digital es válida (González, 2007).

La firma digitalizada, a pesar de que muchas personas la confunden con la firma digital, alude a una mera representación gráfica de una firma hológrafa procesada por un escáner, que puede ser insertada como imagen a un documento o mail. En la tabla 1 se detallan las diferencias entre las firmas, exceptuando la firma digitalizada mencionada.

	Firma Hológrafa	Firma Electrónica	Firma Digital
Unicidad	Única para el firmante	Única para el firmante	Única para el documento
Autenticidad	Puede ser falsificada con facilidad	Puede ser falsificada con facilidad	La persona que firma el documento es quien dice ser y su firma no puede ser falsificada, ni trasladada a otro documento
Integridad	La información puede ser alterada después de ser firmada	La información puede ser alterada antes o después de ser firmada	El mínimo cambio en el documento elimina automáticamente la firma digital. El documento firmado es inalterable
No repudio	Necesita un grafólogo	Corresponde al firmante comprobar o no la validez de la firma	Corresponde a quien invoca la autenticidad de la firma comprobar su validez. La persona que firma no puede declamar el no haber efectuado la firma.

Legalidad	Cuenta con marco legal	No cuenta con marco legal en Argentina	Aprobada por Ley 25506. Tiene la misma validez legal que la firma hológrafa

Tabla 1: Comparación de las firmas

3.4 Identidad digital

Por un lado, el hecho de que una clave sea pública, y que por tanto no sea necesario acceder a ella haciendo uso de un canal adicional, no implica que ésta sea auténtica. Es decir, resulta vital tener la certeza de que la clave pública pertenece a la entidad con la cual se desea establecer contacto. Un error en la asociación entre la identidad del usuario y el valor de su clave pública puede conllevar la transmisión de información sensible a terceras partes o la asociación de cierta información a la entidad equivocada (Reverte, 2002, p.8).

Por otro lado, un individuo, en el proceso de autenticar un documento firmado digitalmente debe conocer la llave pública del supuesto firmante. Asimismo, si un documento es firmado por 10 individuos deberá contar con 10 archivos o con una base de datos, que contenga las 10 llaves públicas de los posibles firmantes. Si este número crece a cien, mil o a un millón, el problema aumenta considerablemente también.

Una solución a la necesidad de asociar de forma confiable las claves públicas de los usuarios a su identidad, se basa en el concepto de la certificación digital.

3.4.1 Certificado Digital

Los certificados digitales son esencialmente tarjetas de identificación de confianza, como lo son los documentos de identidad, pasaportes o licencias de conducir, que están en formato electrónico y vinculan la clave pública de una persona o entidad con información propia de su identidad.

Un certificado digital es emitido por una autoridad, conocida como una Autoridad Certificadora (AC) que garantiza la validez de la información contenida en dicho certificado. En otras palabras, un certificado digital es esencialmente una clave pública y un identificador, firmados digitalmente por una AC, y su utilidad es demostrar que una clave pública pertenece a un usuario concreto. Evidentemente, la citada AC debe encargarse de verificar previamente que la clave pública del usuario es auténtica, otorgando así la confianza correspondiente a las claves públicas asociadas sus certificados emitidos.

3.4.1.1 Estándar X.509

Para definir y establecer el contenido y estructura que debe tener un certificado digital se estableció el estándar conocido normalmente como X.509, aunque su nombre completo es “Internet X.509 Public Key Infrastructure Certificate and

Certificate Revocation List (CRL) Profile". El estándar surgió originalmente en el año 1988 y la última versión vigente, X.509 v3, se aprobó en 2008. Actualmente es el estándar más extendido y utilizado.

Los elementos del formato de un certificado X.509 v3 son:

- Versión: indicador de la versión del certificado (en este caso, versión 3).
- Número de serie: identificador único del certificado, asignado por la autoridad emisora del mismo.
- Algoritmo de la firma: Identificador del algoritmo empleado para firmar digitalmente el certificado
- Nombre del certificador: nombre de la entidad emisora del certificado
- Período de validez: período durante el cual el certificado se considera válido, salvo revocación.
- Nombre del sujeto: nombre de la entidad poseedora de la clave privada que está asociada a la clave pública contenida en el certificado.
- Clave pública del sujeto.
- Identificador único del certificador.
- Identificador único del sujeto.
- Extensiones: las extensiones tienen un tipo asociado, que debe ser registrado mediante la asignación de un identificador único de objeto (OID, Object IDentifier), un indicador acerca de la criticidad y un valor
- Firma digital de todo lo anterior generada por el certificador.

De las especificaciones del estándar X.509 nace el concepto de infraestructura de clave pública (PKI, Public Key Infraestructure), que hace referencia al conjunto de elementos y procedimientos relacionados con la gestión del ciclo de vida de un certificado digital. Las infraestructuras de clave pública son elementos clave a la hora de dotar al sistema de la capacidad de gestionar todos aquellos aspectos implicados en la creación, publicación, renovación, validación y revocación de certificados (Reverte, 2002, p.8).

3.4.2 Infraestructura de Clave Pública

También llamada Infraestructura de Firma Digital, una PKI puede ser definida como un conjunto de recursos de software, hardware y humanos que posibilitan el uso de la criptografía de clave pública para proporcionar servicios básicos de seguridad de confidencialidad, autenticación, integridad y no repudio. En conjunto ayudan a facilitar el almacenamiento y el intercambio de datos electrónicos de una manera segura.

Una PKI contiene cinco tipos de elementos:

- Autoridad de Certificación o Autoridad Certificante (AC): es la entidad principal del sistema, encargada de tramitar todas las solicitudes relacionadas con el ciclo de vida de los certificados digitales. Emite los certificados digitales, firma las listas de certificados revocados (CRL por sus siglas en inglés) y las políticas de certificación, y publica la información generada en los repositorios de datos tanto internos como externos.
- Autoridad de Registro (AR): Normalmente es la primera entidad de contacto con la infraestructura de certificación. Es una entidad certificada por la AC que actúa como interfaz entre los clientes y la propia AC. Es usual utilizar una o varias AR subordinadas a una AC cuando ésta atiende solicitudes de un área compleja o grande. Si en una implementación de una PKI se decide no utilizar una AR, entonces las funciones de esta pasarían a la AC.
- Usuarios finales de los certificados: son los que pueden firmar documentos digitalmente y descifrarlos usando sus claves privadas.
- Repositorios: almacenan y publican los certificados y listas de certificados revocados.
- Los certificados digitales.

La figura 6 ilustra la relación existente entre estos elementos, las operaciones que pueden ser solicitadas por partes de los usuarios finales y las distintas funciones asociadas a cada uno de los elementos de gestión.

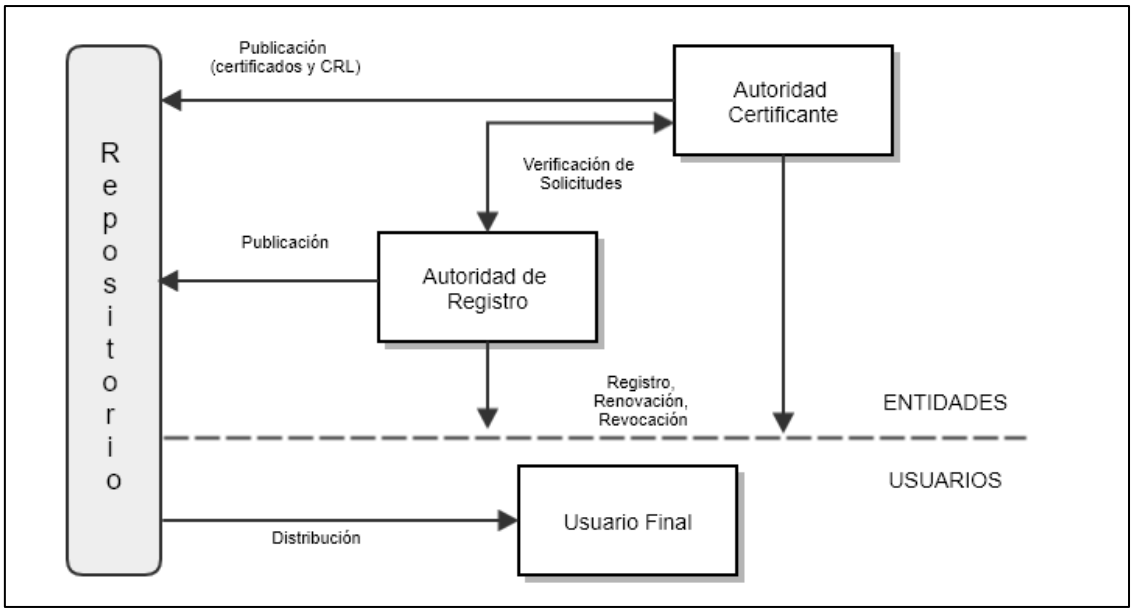


Figura 6: Elementos de una PKI

Si bien estos son los elementos de una PKI, no significa que sean limitantes o únicos. Puede existir una jerarquía entre más de una AC. En esta modalidad, las

AC se organizan en forma de árbol por niveles, de tal manera que las AC de un nivel poseen certificados digitales emitidos por autoridades de niveles superiores. De esta forma, es posible la verificación satisfactoria de un certificado digital cualquiera, siempre que poseamos la clave pública de un certificador de primer nivel (denominados “hojas”).

Para comprobar la integridad de un certificado se verifica la firma realizada por su AC correspondiente, repitiendo el proceso para la AC padre y así sucesivamente hasta alcanzar la entidad de confianza raíz. La AC Raíz es el elemento inicial de la jerarquía y su confianza se basa en la autofirma de su certificado digital.

Como es natural, las AC que generen certificados finales, correspondientes a las hojas del árbol, tendrán la única responsabilidad de comprobar de manera fehaciente que cada clave pública pertenece a su propietario. Sin embargo, aquellas entidades que certifiquen a otras entidades deberán garantizar, además, que estas últimas emplean mecanismos adecuados para comprobar las identidades de sus clientes. De lo contrario, alguien podría crear una AC, obtener el correspondiente certificado digital de niveles superiores, y luego emitir certificados falsos. Si bien el esquema jerárquico es realmente simple y efectivo, presenta un problema importante: si uno de los certificadores resulta comprometido, todos sus descendientes en el árbol quedan invalidados. Esto obliga, por un lado, a que las AC sean lo más transparentes posible, y por otro a que se mantengan siempre al día las listas de revocación de certificados (Lucena López, 2010, p.236).

3.4.3 Ciclo de vida del certificado digital

La figura 7 ilustra el ciclo de vida de un certificado digital abarcando todas aquellas operaciones de gestión de información contenida en el mismo realizadas por los distintos elementos que componen una PKI.

El proceso de generación de claves criptográficas requiere aleatoriedad, de forma que el par de claves generado no sea fácilmente predecible. Una vez generado el par de claves, es necesario proteger convenientemente la clave privada, ya que la aplicabilidad de los certificados digitales recae en el hecho de que ésta sólo sea utilizada por la persona a la cual pertenece. Normalmente, los métodos empleados para proteger las claves privadas son:

1. Almacenamiento por hardware, ya sea en una tarjeta inteligente o dispositivo de almacenamiento masivo (USB Token).
2. Almacenamiento por software, es decir, en un fichero cifrado contenido en el disco duro de la computadora.
3. Almacenamiento por servidor de credenciales, el cual se encarga de distribuir la clave privada al usuario después de haberlo autenticado.

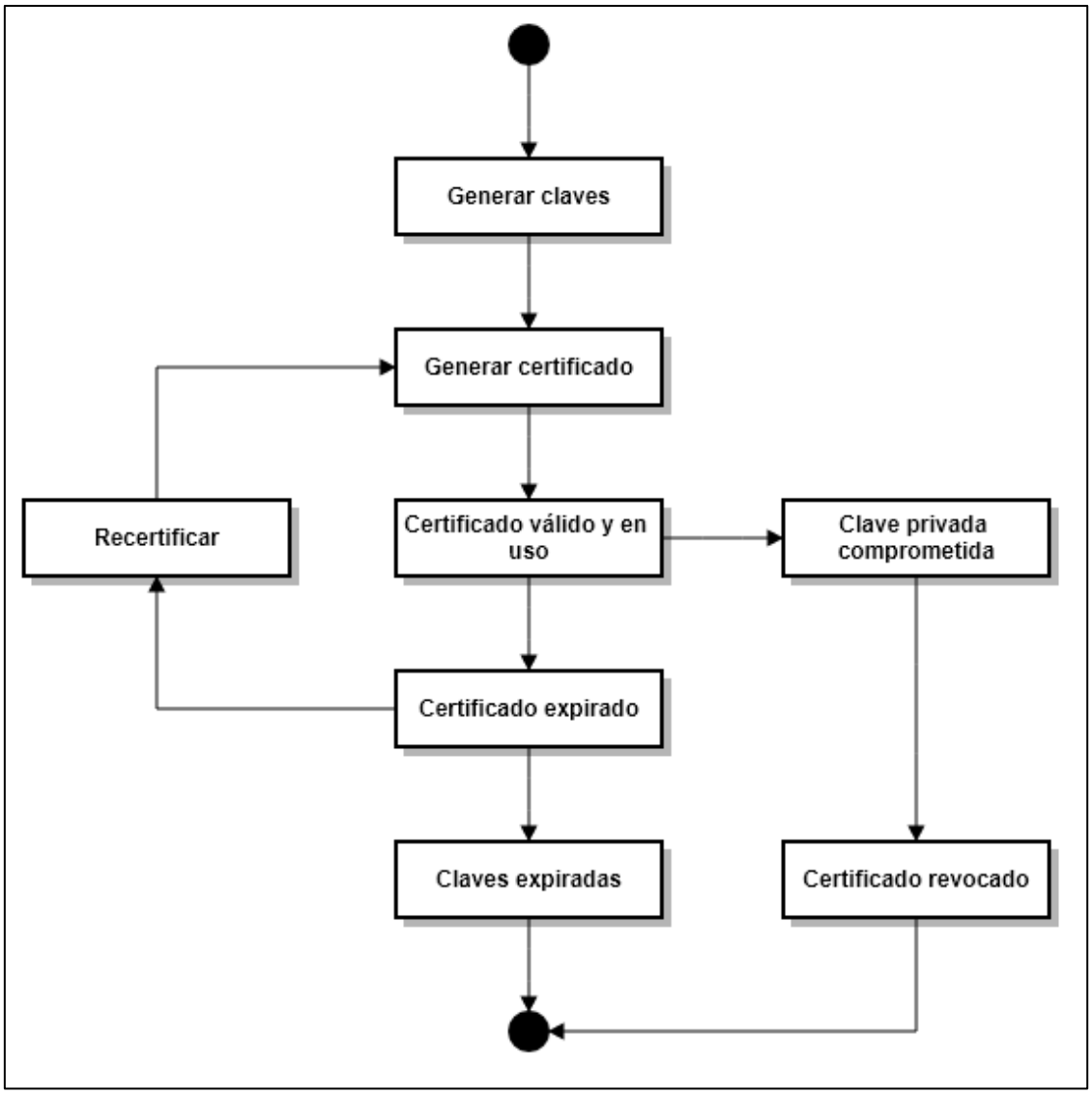


Figura 7: Ciclo de vida del certificado digital

La generación de los certificados se realiza mediante las AR, que son las encargadas de interactuar entre la AC y los usuarios finales. Si bien, las AR simplemente validan o rechazan las solicitudes mediante documentos acreditativos presentados en forma personal, las AC son las encargadas de emitir y publicar todas aquellas solicitudes.

Los certificados tienen un tiempo de vida limitado y, en general, deben ser renovados tras su expiración. Dicha renovación puede conllevar, también, a un cambio de pares de claves, aunque no siempre es obligatorio, ya que es posible emitir nuevos certificados que incluyan las claves contenidas previamente en certificados que caducaron.

Si bien se espera que los certificados sean usados en el período de validez, algunos usuarios se ven obligados, bajo ciertas circunstancias, a dejar de confiar en las claves antes de que estas caduquen. Tales circunstancias incluyen el

conocimiento o sospecha del compromiso de una clave privada, el cambio de nombre, o el cambio de relación entre la entidad certificada y la AC. En estos casos, se debe revocar el certificado. La AC es la responsable de dicha función, bajo previa solicitud y evaluación de la AR.

Todos los procesos, incluido la lista de certificados revocados (CRL, Certificate Revocation List), deben ser comunicados y propagados por la AC con el fin de evitar que algún certificado en cuestión se siga empleando (Reverte, 2002).

3.5 Dispositivos criptográficos (Tokens)

Si bien anteriormente se mencionó el nombre de dispositivo criptográfico o USB token, es objetivo de este apartado definirlo correctamente.

Un Token USB (a veces token de autenticación o de seguridad) es un dispositivo físico que un usuario autorizado utiliza para facilitar la autenticación a algún servicio informático. Es decir, establece una identidad personal sin la necesidad de acceder con una contraseña. En la criptografía de clave pública, un token USB se utiliza para almacenar un certificado digital.

Entre las características de un token, se pueden destacar las siguientes:

- La clave privada es almacenada por el token e impide que se recupere fuera del mismo. Esto permite que la creación de la firma digital se realice en el token.
- Ciertos tokens pueden almacenar datos biométricos, como huellas dactilares.
- Existen tokens que incluyen pequeños teclados para permitir la entrada de un PIN.
- Utilizan el puerto USB o conectividad Bluetooth como medio de transferencia de información.
- Tienen tamaño pequeño, como un llavero o accesorio de bolsillo.
- Son duraderos y confiables.
- En la mayoría de los casos, no requieren controladores de software (drivers) adicionales. Son dispositivos *Plug and Play*.

3.5.1 Regulación de dispositivos criptográficos

FIPS, acrónimo de Federal Information Processing Standard (estándares federales de procesamiento de la información), publicación 140-2, es una norma gubernamental de EE. UU. que describe el cifrado y los requisitos de seguridad relacionados que los productos de TI deben cumplir para el uso con datos sensibles, pero no clasificados. La norma garantiza que un producto usa prácticas de seguridad sólida, tales como métodos y algoritmos, de cifrado,

aprobados y de alta seguridad. También especifica cómo particulares u otros procesos deben estar autorizados para utilizar el producto y cómo se deben diseñar los módulos o componentes para interactuar de manera segura con otros sistemas (Seagate, s.f.).

FIPS 140-2 define cuatro niveles de seguridad:

- El **nivel 1** típicamente se usa para productos de cifrado sólo para software, impone requisitos de seguridad muy limitados. Todos los componentes deben ser de nivel de producción y los diversos tipos flagrantes de inseguridad deben estar ausentes.
- El **nivel 2** requiere la autenticación basada en la función. (No se necesita la autenticación de usuario particular.) También requiere la capacidad de detectar la violación física mediante el uso de bloqueos físicos o sellos a prueba de violaciones.
- El **nivel 3** agrega violación física resistencia al desmontaje o modificación, haciéndolo extremadamente difícil para sabotear. Si se detecta una violación, el dispositivo debe ser capaz de borrar los parámetros de seguridad críticos. El nivel 3 también incluye una sólida protección de cifrado y administración de claves, autenticación basada en la identidad, así como la separación física o lógica entre las interfaces mediante el ingreso y la salida de los parámetros de seguridad críticos.
- El **nivel 4** incluye una protección avanzada contra violación y está diseñado para ser utilizado con productos que operan en ambientes desprotegidos físicamente.

El Instituto Nacional de Estándares y Tecnología, o NIST (por sus siglas en inglés), estableció el Programa de validación de módulos de cifrado (CMVP), el cuál verifica que un producto cumpla con la norma FIPS 140-2, especificando también su nivel de seguridad (Seagate, s.f.).

Para verificar la información sobre dispositivos criptográficos validados por NIST, se debe ingresar a:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search

Capítulo 4: Marco teórico-legal en Argentina y el Mercosur

Este capítulo se centrará en el marco legal de la firma digital en Argentina, las leyes que la contemplan y las entidades que interactúan en la Infraestructura de Firma Digital de la nación. Se inicia con un enfoque detallado de la firma digital, su importancia y definición según el Mercado Común del Sur, hasta llegar a la ley nacional de firma digital N° 25506. Se hará una cronología de la mencionada ley y un breve relevamiento del caso en la provincia de San Luis, cuna del crecimiento digital de Argentina.

4.1 Los enfoques de la firma digital

Para garantizar las operaciones realizadas por medios electrónicos, las organizaciones, tanto públicas como privadas, necesitan contar con procedimientos que identifiquen a los usuarios. Este concepto de autenticación puede ser analizado desde dos puntos de vista. Por un lado, el enfoque tecnológico, es decir, las herramientas que se utilizan en el entorno digital para identificar a las personas ante los sistemas informáticos. Por otro, el enfoque jurídico, es decir, la naturaleza jurídica que tiene cada una de las opciones tecnológicas elegidas para identificar a las personas.

Si estos conceptos se trasladan específicamente a la firma digital, el enfoque tecnológico hace uso de la criptografía asimétrica y las funciones hash para establecer claves compartidas o, en esquemas más complejos, conocidos como infraestructura de clave pública, la generación de certificados digitales. Por su parte, el enfoque jurídico se centra en la equivalencia funcional y legal de la firma digital con respecto a la hológrafa, bajo las características de expresión del consentimiento de una persona con un determinado acto jurídico y el contenido de un documento.

4.2 Marco legal en el Mercado Común del Sur

El Mercado Común del Sur (MERCOSUR) es un proceso abierto y dinámico de integración regional instituido inicialmente por Argentina, Brasil, Paraguay y Uruguay (denominados Estados Partes) al cual, en fases posteriores, se han incorporado Venezuela (actualmente suspendida) y Bolivia (ésta última en proceso de adhesión). Desde su creación, en 1991, tuvo como objetivo principal propiciar un espacio común que generara oportunidades comerciales y de inversiones a través de la integración competitiva de las economías nacionales al mercado internacional. Como resultado ha establecido múltiples acuerdos con países o grupos de países, otorgándoles, en algunos casos, carácter de Estados Asociados. Entre ellos se pueden encontrar Chile, Ecuador, Perú, Colombia, Guyana y Surinam (Sitio web institucional Mercosur - En pocas palabras, s.f.).

En 2006, bajo el enfoque de firma digital, el Mercosur aprueba dos leyes pertinentes al tema de autenticación. La primera de ellas, la Resolución GMC N° 34/06, establece las directrices a ser consideradas en futuros acuerdos de reconocimiento de certificados emitidos por los países miembros entre sí. Establece estándares a ser tenidos en cuenta enfocándose, asimismo, en los criterios de seguridad física y lógica de los prestadores de servicios de certificación, los criterios de auditoría y los controles aplicables a los certificadores, los criterios de emisión de certificados reconocidos y hasta recomendaciones para la verificación segura de firmas digitales (o firmas electrónicas avanzadas, según otros países). En términos generales, esta Resolución no toma en consideración el distinto enfoque que cada país ha dado al tema de infraestructura de clave pública.

La segunda, la Resolución GMC N° 37/06, contempla la eficacia jurídica del documento electrónico, de la firma electrónica y de la firma digital en el ámbito del Mercosur. Dispone que, en cualquiera de los Estados Partes, los documentos electrónicos tendrán los mismos efectos jurídicos que los documentos escritos, salvo excepciones contempladas en las legislaciones nacionales. Reconoce la validez de la firma electrónica cuando la misma fuese admitida como válida por las partes que la utilizan. Por otra parte, para el reconocimiento de la firma digital y sus certificados se realizan los llamados acuerdos de reconocimiento. Dichos acuerdos otorgan a las firmas digitales, que cumplan con las condiciones dispuestas en ellos, el mismo valor jurídico y probatorio que el otorgado a las firmas manuscritas. De esta manera, los Estados Partes reconocen la autenticidad e integridad de un documento electrónico con firma digital. (Resolución GMC N° 37/06, 2006, art. 4°).

Sin embargo, ninguna de estas Resoluciones tiene efecto práctico, por cuanto la primera, si bien no requiere la incorporación al derecho interno, no establece un acuerdo de reconocimiento, sino que fija pautas a tal fin. La segunda, por su parte, requiere de su incorporación al derecho interno para tener eficacia jurídica, con lo cual, representa solamente una declaración general sin efectos jurídicos (Rivolta & Bugoni, 2007, p.46).

4.2.1 Definiciones según el Mercosur

Para el Mercosur, la firma electrónica es un conjunto de datos, en forma electrónica, anexos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados por el firmante como medio de identificación. De la misma manera, define a la firma digital como una firma electrónica que cumple con los siguientes requisitos:

- Requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca.
- Ser creada por medios que el firmante pueda mantener bajo su exclusivo control;

- Ser susceptible de verificación por terceros
- Estar vinculada a estos datos de tal modo que cualquier alteración subsiguiente en los mismos sea detectable.
- Haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido y válido al momento de la firma (Resolución GMC N° 37/06, 2006, Art.3).

4.2.2 Mercosur Digital

Mercosur Digital fue un proyecto de cooperación internacional entre la Unión Europea y el MERCOSUR, que nació con el objetivo de reducir las asimetrías legales y tecnológicas entre ambas regiones en el período comprendido en los años 2009 y 2010. Además, buscaba promover políticas y estrategias comunes en el área de la Sociedad de la Información para contribuir al crecimiento, la integración económica y el desarrollo del comercio electrónico en Argentina, Uruguay, Brasil y Paraguay (los Estados Partes en ese momento) por medio de la armonización de las regulaciones, la implementación de la infraestructura tecnológica y el intercambio de conocimientos. La figura 8 y 9 muestran el presupuesto del proyecto durante abril de 2009 a diciembre de 2010.

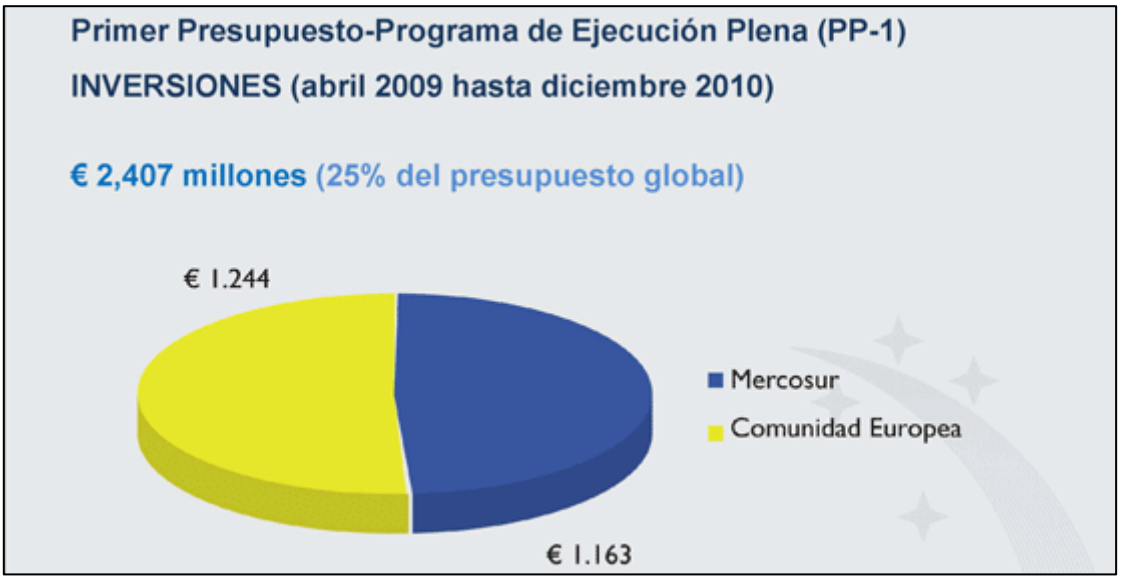


Figura 8: Inversiones de Mercosur Digital (Blanco, 2011)

Si bien el tema principal era la creciente demanda del Comercio Electrónico, también se elaboró un Plan Director de Certificación Digital para el Mercosur, con definición del modelo tecnológico de integración de las infraestructuras de clave pública de los países y la definición del modelo tecnológico y jurídico de integración y reconocimiento de las firmas digitales en los cuatro países,

viabilizando el aumento de credibilidad en las comunicaciones y transacciones de negocio entre los países del Mercosur y del resto del mundo.

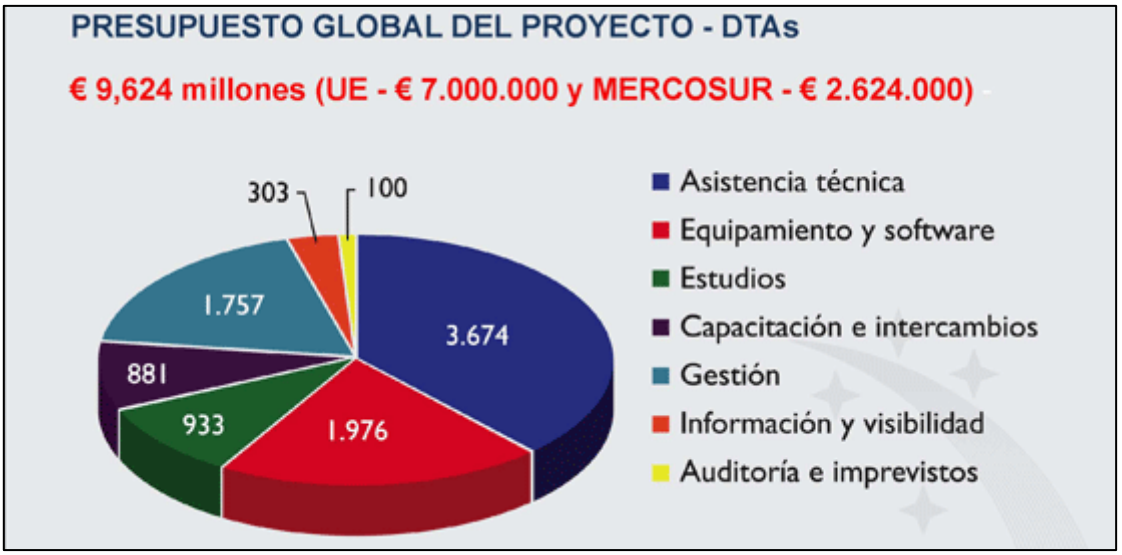


Figura 9: Presupuesto Global de Mercosur Digital por rubro (Blanco, 2011)

Los Estados Parte Uruguay y Paraguay tuvieron avances significativos, pudiendo de esta forma crear sus infraestructuras de clave pública. Por su parte Argentina obtuvo fondos para complementar su infraestructura de clave pública y proveer, junto a Uruguay, la infraestructura básica de sello de tiempo (Time Stamping) con el objeto de que ambos países brinden ese servicio. Time-Stamping (TS) es la tecnología que permite demostrar que una serie de datos han existido y no han sido alterados desde una fecha y hora determinada. Esto es válido de aplicar en operaciones electrónicas, movimientos, modificaciones y/o consultas de información dentro de un sistema informático (Nishikawa & Matsuoka, 2008).

En resumen, los logros del proyecto pueden ser clasificados en dos grandes categorías: *Infraestructuras*, que comprenden todos los equipamientos, sistemas y consultorías contratados para promover el comercio electrónico en los cuatro países miembros; y *Estudios y Diagnósticos en el Mercosur*, que comprenden los nuevos recursos (legales, autorizaciones, normas) para el apoyo o realización del comercio electrónico y la infraestructura de TICs en el Mercosur. Dichos estudios se centraron en temas específicos como:

- Ecosistema de comercio electrónico y negocios por Internet transfronterizo.
- Generación de confianza en internet, oferta y demanda de productos y servicios susceptibles para el comercio electrónico y negocios por Internet transfronterizos

- Elaboración de un Plan Director de comercio electrónico y negocios por Internet para el Mercosur y la formación y capacitación para las pequeñas y medianas empresas (PyMES) (Mercosur Digital, 2013).

4.3 Marco legal en Argentina

Argentina cuenta con un marco normativo completo en materia de transacciones electrónicas. La ley de Firma Digital N° 25506 habilita el uso del documento electrónico, la firma electrónica y la firma digital en todo el territorio nacional. Es una ley que complementa las disposiciones del Código Civil, con el objetivo de facilitar el uso de medios digitales para la realización de transacciones, tanto entre particulares como parte de los organismos del Estado.

4.3.1 Un poco de historia

Argentina, una de las naciones más activas en el desarrollo de la infraestructura de firma digital en el ámbito latinoamericano, formuló en 1998, el Decreto N° 427/1998, que aprobaba la creación de una infraestructura de clave pública para el Sector Público Nacional en un plazo de máximo de dos años a partir de esa fecha. En efecto, las normas de ese momento se basaban en criterios tecnológicos que rápidamente fueron superados con el paso del tiempo, ya que los procesos de aprobación legislativa no avanzan con la misma celeridad que la tecnología. A pesar de que, en el año 2001, bajo la Decisión Administrativa N° 102/2000, se prorroga la implementación de la firma digital por dos años más, se ve reflejada la necesidad de contar con leyes tecnológicamente neutras, es decir, que sobrevivan a los avances de la tecnología.

Con el objetivo de solventar el problema del incesante avance de la tecnología, a fines del año 2001, sin haber implementado todavía la infraestructura de firma digital en Argentina, se sanciona la vigente Ley N° 25506 de Firma digital, que posteriormente fue reglamentada por el Decreto N° 2628/2002 y sus modificaciones. Dicha ley, que reconoce como antecedente al decreto de 1998, en su Art. 48° menciona que, en un plazo máximo de 5 años, contados a partir de su entrada en vigencia, se pretende llevar a cabo nuevamente la implementación de la infraestructura. Es decir que para diciembre de 2006 se esperaba la aplicación de la firma digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias según el art. 8° de la ley 24156. Sin embargo, esto no ocurrió así.

Finalmente, durante el año 2007, se establece un marco normativo de firma digital aplicable al otorgamiento y renovación de las licencias a los certificadores que así lo soliciten y se aprueba, a su vez, la política de certificación de la Autoridad Certificante Raíz de la República Argentina, logrando la tan ansiada implementación de la infraestructura de la firma digital. A pesar de ello, no fue hasta el año 2015, cuando el tema se incorpora al nuevo Código Civil obteniendo

de esta forma, la firma digital, la misma validez legal que la que tiene la firma holográfica (Carbone, 2016).

La tabla 2 muestra en orden cronológico el marco legal con respecto a la firma digital en Argentina.

Normativa	Fecha	Descripción	Modifica o deroga
Decreto N° 427/1998	16 de abril de 1998	Creación de una PKI para el Sector Público Nacional. Aprueba un plazo de 2 años para su implementación	
Decisión Administrativa N° 102/2000	25 de enero de 2001		El Art. 1° prorroga el Art. 1° del Decreto N° 427/1998 por 2 años a partir del 31 de diciembre de 2000
Ley Firma Digital N° 25506	14 de noviembre de 2001 (vigente)	Reconoce y establece las condiciones para el empleo de la firma electrónica y de la firma digital y su eficacia jurídica, y crea la Infraestructura de Firma Digital de la República Argentina.	El Art. 48° da un plazo máximo de 5 años contados a partir de la entrada en vigencia de la presente ley.
Decreto N° 2628/2002	19 de diciembre de 2002 (vigente)	Un reglamento que regula el empleo de la firma electrónica y de la firma digital y su eficacia jurídica.	
Decisión Administrativa 06/2007	07 de febrero de 2007	Establece un marco normativo de firma digital aplicable al otorgamiento y renovación de las licencias a los certificadores que así lo soliciten	Deroga al Decreto N° 427/1998
Resolución SGP N° 63/2007	13 de noviembre de 2007	Aprueba la política única de certificación de la AC-RAÍZ de la República Argentina	
Decisión Administrativa N° 927/2014	30 de octubre de 2014		Deroga la Decisión Administrativa N° 06/2007
Disposición SSTG N° 07/2015	10 de septiembre de 2015	Aprueba aclaraciones técnicas específicas para la Decisión Administrativa N° 927/2014	
Resolución MM N° 399-E/2016	05 de octubre de 2016 (vigente)	Establece los procedimientos y condiciones que se deberán cumplir para emitir certificados digitales en el ámbito de la PKI en la República Argentina	Reemplaza la Decisión Administrativa N° 927/2014 y la Disposición SSTG N° 07/2015
Resolución MM N° 37-E/2016	20 de diciembre de 2016 (vigente)	Aprueba la política única de certificación de la AC-RAÍZ de la República Argentina V2.0	Deja obsoleta la Resolución SGP N° 63/2007
Resolución MM N° 213-E/2017	05 de septiembre de 2017 (vigente)		Modifica el Art. 6° de la Resolución MM N° 399-E/2016
Decreto MM N° 892/2017	01 de noviembre de 2017 (vigente)	Creación de una Plataforma de Firma Digital Remota	
Resolución SMA Nº 116-E/17	15 de diciembre de 2017 (vigente)	Exigencia a certificadores licenciados y sus autoridades de registro. Captura de fotografía digital del rostro y la huella dactilar de los	

		solicitantes y suscriptores de certificados de firma digital.	

Tabla 2: Breve descripción de la cronología normativa de la firma digital en Argentina

4.3.2 La firma digital según la ley nacional

La ley nacional de firma digital, definida en once capítulos y un anexo, establece definiciones en relación con su alcance, validez y presunciones legales como la autoría e integridad de la firma digital.

El Decreto N° 427/1998 definía a la firma digital como el resultado de una transformación de un documento digital empleando un criptograma asimétrico y un digesto seguro (o función hash), de forma tal que una persona que posea el documento digital inicial y la clave pública del firmante pueda determinar con certeza:

1. Si la transformación se llevó a cabo utilizando la clave privada que corresponde a la clave pública del firmante;
2. Si el documento digital ha sido modificado desde que se efectuó la transformación.

La conjunción de los dos requisitos anteriores es la garantía de su no repudio y su integridad (Decreto N° 427/1998, 1998, Anexo II). Esta definición, si bien es acertada, fue mutando hasta la que se conoce hoy en día.

Según la ley vigente, 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 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. Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes (Ley N° 25506, 2001, art. 2°).

Si cumple los requisitos planteados anteriormente, este mecanismo de autenticación será considerado ante la ley como firma digital y gozará de dos presunciones asociadas, la presunción de autoría del documento electrónico, y la presunción de integridad de los contenidos del mismo. Estas presunciones son *iuris tantum*, es decir, que se admiten salvo que se pruebe lo contrario. Así mismo, si alguno de los requisitos que exige la ley para considerarla firma digital no se cumpliera, entonces tendrá el valor de una firma electrónica, pues ha sido utilizado mediante acuerdo de partes para identificarse en el entorno digital y para expresar su consentimiento con el contenido del documento electrónico firmado.

Por otra parte, la ley establece que cuando se requiera una firma manuscrita, esta podrá ser satisfecha por una firma digital, siendo válida si se crea durante

la vigencia del certificado digital del firmante, emitido por un certificador licenciado y posteriormente sustentable a verificación (Rivolta & Bugoni, 2007, p.55).

4.4 Infraestructura de clave pública en Argentina

Como se mencionó anteriormente, Argentina ha sido un país pionero en la materia. El Decreto N° 427/1998 autorizaba el uso de la firma digital en el ámbito del sector público nacional y se creaba, de esta manera, la primera reglamentación para la Infraestructura de Firma Digital para la Administración Nacional. Cuando se sanciona la ley N° 25506 de firma digital, a fines del 2001, se amplía el alcance de la infraestructura a todo el territorio nacional.

De esta manera, Argentina, define a su infraestructura de clave pública como al conjunto de servidores y otros equipamientos informáticos relacionados, software y dispositivos criptográficos utilizados para la generación, almacenamiento, publicación y posterior consulta de validez de los certificados digitales. Es decir, la Infraestructura de Firma Digital de la República Argentina (IFDRA) está conformada por un conjunto de componentes que interactúan entre sí, permitiendo la emisión de certificados digitales para verificar firmas en condiciones seguras, tanto desde el punto de vista técnico como legal (Ente Licenciante - Argentina, s.f.).

4.4.1 Elementos de la IFDRA

Los elementos de una infraestructura de clave pública pueden ser: Autoridades Certificantes, Autoridades de Registro, certificados digitales, usuarios finales y los repositorios. Si bien estos elementos varían de acuerdo con las leyes de los distintos países, en Argentina, la IFDRA se compone de la siguiente manera:

i. El ente licenciante (también conocido en la ley como Autoridad de Aplicación) y su Autoridad Certificante Raíz.
ii. Los certificadores licenciados, incluyendo sus autoridades certificantes y sus autoridades de registro, según los servicios que presten.
iii. Las autoridades de sello de tiempo.
iv. Los suscriptores de los certificados.
v. Los terceros usuarios, según lo dispuesto en el Anexo I del Decreto N° 2628/02 y sus modificatorios.
vi. Los certificadores reconocidos por la Autoridad de Aplicación.

4.4.1.1 Ente licenciante

Es el organismo con carácter técnico administrativo que regula la IFDRA. En un principio, la Ley N° 25506 asigna a la Jefatura de Gabinete de Ministros del gobierno federal, las funciones de autoridad de aplicación, quedando relegada en el 2005 por el Decreto N° 409 de dicho año, quien asignaba el rol a la

Subsecretaría de la Gestión Pública, dependiente de Jefatura de Gabinete de Ministros de la nación. Actualmente, el Ministerio de Modernización actúa como Ente Licenciante otorgando, denegando o revocando las licencias de los certificadores licenciados y supervisando su accionar.

Por otro lado, la Autoridad Certificante Raíz (AC-RAIZ) es la Autoridad Certificante administrada por la Secretaría de Modernización Administrativa perteneciente al Ministerio de Modernización. Constituye la única instalación de su tipo y reviste la mayor jerarquía de la IFDRA. Es encargada de emitir certificados digitales a las Autoridades Certificantes de los certificadores licenciados, una vez aprobados los requisitos de licenciamiento establecidos en la ley N° 25506 (Resolución MM N° 399-E/2016, 2016, art. 14°).

4.4.1.2 Autoridades Certificantes

La Ley de firma digital establece un sistema de licenciamiento voluntario para aquellas empresas o entidades que emitan certificados digitales cuyo valor legal sea de una firma digital. Cabe hacer la aclaración de que las empresas que emitan certificados digitales que no vayan a ser utilizados para firmar digitalmente, no requieren de autorización o licenciamiento estatal. Esto podría darse, por ejemplo, para las empresas que emiten certificados de servidores, o certificados digitales para personas que firmen documentos electrónicos, pero con valor legal de firma electrónica (Rivolta & Bugoni, 2007, p.86-87).

En el art. 17°, la ley establece que pueden ser certificadores licenciados las personas de existencia ideal, los registros públicos de contratos, más conocidos como Escribanos Públicos o Notarios, y los organismos públicos que expidan certificados, presten otros servicios en relación con la firma digital y cuenten con una licencia para ello, otorgada por el ente licenciante. Por otra parte, la ley no permite que una persona física ejerza la calidad de certificador licenciado.

Para poder emitir certificados digitales que puedan ser utilizados para firmar con los efectos jurídicos de una firma digital, los certificadores deben contar con una licencia especial otorgada por el Ministerio de Modernización, en su calidad de autoridad de aplicación de la ley. Para obtener dicha licencia, el certificador debe cumplir con los requisitos establecidos por la ley y tramitar la solicitud respectiva ante el ente licenciante, el que otorgará la licencia previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones. La ley establece que dichas licencias no pueden ser transferibles.

Hoy en día, la IFDRA cuenta con 11 autoridades certificadoras[8] (incluida la AC-RAÍZ) y 5 entidades en proceso de licenciamiento[9].

[8] Para más información consultar https://www.acraiz.gob.ar/Home/PoliticasDeCertificacion
[9] Para más información consultar https://www.acraiz.gob.ar/Home/SolicitantesDeLicencias

4.4.1.3 Autoridades de Registro

Los Certificadores Licenciados podrán delegar a entidades facultadas, denominadas Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptores de certificados y de registro de las presentaciones y trámites que les sean formuladas, bajo su responsabilidad, cumpliendo las normas y procedimientos establecidos en el Decreto N° 2628/2002. Así mismo, una Autoridad de Registro puede constituirse como una única unidad o con varias unidades dependientes jerárquicamente entre sí, pudiendo, delegar su operatoria en otras autoridades de registro, siempre que medie la aprobación del Certificador Licenciado (Decreto N° 2628, 2002, Art. 36°).

4.5 Infraestructura de firma digital de San Luis

En una entrevista para CanalAR[10], Marcos Hauria, exdirector del Instituto de Firma Digital de la Provincia de San Luis (febrero 2014), menciona que, desde la sanción de la ley nacional de firma digital a la actualidad, IFDRA ha tenido una implementación por parte de las provincias que se ha visto ralentizada por distintos factores, a excepción de la provincia de San Luis, que se ha convertido en referente nacional, marcando el rumbo a seguir en la materia (Hauria, 2014).

A raíz de ello, en 2007, la provincia de San Luis sanciona su propia ley provincial de Firma Digital mediante la cual se adhiere a la Ley Nacional Nº 25506, instrumentando los recaudos necesarios para establecer dentro de su jurisdicción la operatividad de los actos y mecanismos previstos en los Capítulos I a IV de la Ley Nacional de referencia. De esta manera, se crea el Instituto de Firma Digital de San Luis (de ahora en más FDSL) el cual opera de forma paralela al IFDRA, quedando el país divido en dos entes licenciantes no relacionados entre sí.

El FDSL, perteneciente a la Agencia San Luis Ciencia, Tecnología y Sociedad, es una repartición del Gobierno de la provincia de San Luis, creada en el año 2009 bajo el programa San Luis Digital, a fin de realizar dos importantes tareas vinculadas con la gestión de firma digital:

1. Como Ente Licenciante Provincial, FDSL es el órgano administrativo encargado de otorgar las licencias a aquellos que deseen constituirse como Certificadores Licenciados Provinciales.
2. Como Certificador Licenciado Provincial, FDSL cuenta con seis Autoridades Certificantes a través de las cuales emite certificados de firma digital actuando como una Tercera parte confiable.

Desde entonces, FDSL cuenta con una sala cofre de uso exclusivo de la infraestructura provincial de firma digital que, a través del cumplimento con estándares internacionales de seguridad, cuenta con seis niveles de acceso y

[10] CanalAR es el diario digital dedicado a las TICs, la ciencia y la cultura en Argentina.

avanzados medios de identificación, a los que sólo ingresa su personal (Sitio oficial Firma Digital de San Luis 3.0, s.f).

San Luis cuenta con seis Políticas de Certificación vigentes, donde cada una define el ámbito de usabilidad y aplicabilidad del certificado digital, y más de 30 autoridades de registro en el territorio argentino, mayormente entidades del sector privado. Recientemente, en agosto del corriente año, la empresa Camuzzi Gas, la distribuidora de gas más grande de la Argentina, firmó un convenio de cooperación con el FDSL con el objetivo de establecer Autoridades de Registro Remoto para poder emitir certificados de firma digital a sus empleados y autoridades (Agencia de Noticias de San Luis, 2017).

4.6 Relación entre las infraestructuras del país

Como mencionamos anteriormente, por un lado, IFDRA se encuentra bajo la dirección del Ministerio de Modernización y abarca todo el territorio argentino. Por otra parte, FDSL centra su infraestructura en la provincia de San Luis, cuyo ente licenciante lo aplica la Universidad Nacional de La Punta de dicha provincia.

En síntesis, la República Argentina cuenta con dos infraestructuras de firma digital activas, IFDRA e FDSL, y, en consecuencia, aspira lograr un reconocimiento mutuo de los certificados emitidos por ambas jurisdicciones, mejor conocido como certificación cruzada (Hauria, 2014).

Capítulo 5: La solución

Este capítulo está dividido en dos partes. Primero, se detallarán las tareas a llevar a cabo para constituir a la Universidad Nacional de Río Negro (UNRN) como Autoridad de Registro directa de la Oficina Nacional de Tecnologías de Información. Segundo, una vez constituida la Autoridad de Registro, es necesario una reingeniería de procesos considerando el reemplazo progresivo de la documentación en papel y firma hológrafa de los mismos por documentación digital y firma digital, partiendo de las herramientas que se emplean hasta su resguardo. Con respecto a las herramientas se analizarán tanto las funcionalidades como el alcance, mientras que para el resguardo de la información se hará una diferencia entre el repositorio digital con el que cuenta la UNRN y los gestores de contenidos, cuál utilizar y porqué.

5.1 La UNRN como futura Autoridad de Registro

La Oficina Nacional de Tecnologías de la Información (de ahora en más ONTI), Autoridad Certificante que depende directamente de la AC-RAÍZ (como se mencionó en el capítulo anterior), es el organismo referente en la transformación e implementación de soluciones tecnológicas para la Administración Pública Nacional, a fin de promover la integración de nuevas tecnologías, su compatibilidad, interoperabilidad y la estandarización tecnológica.

A fines del año 2015 se crea el Ministerio de Modernización con el objetivo de implementar tecnología para modernizar la administración pública, promoviendo espacios participativos, integradores e inclusivos del ciudadano con el Gobierno. El Ministerio de Modernización cuenta con 4 secretarías, 9 subsecretarías y 69 direcciones. La ONTI, actualmente, es una dirección que pertenece a la Subsecretaría de Tecnologías y Ciberseguridad[11], la cual busca fortalecer la infraestructura tecnológica del Estado Nacional, para brindar servicios seguros, confiables y de calidad a los ciudadanos.

EL “Manual de Procedimientos” y la “Política Única de Certificación” son documentos de la ONTI que brindan especificaciones que debe cumplir toda Autoridad de Registro para formar parte de la infraestructura que provee Argentina en el marco del Sector Público Nacional. Sin embargo, también existe un documento titulado “Requerimientos para la conformación de las Autoridades de Registro de la AC ONTI”, que se basa en los anteriores mencionados y hace hincapié en la formación de una institución como Autoridad de Registro.

En esta sección del capítulo se hará referencia a dichos documentos, con un enfoque más general en el último mencionado, siguiendo los puntos que en ellos se estipulan, con el objetivo de recabar información respecto al estado actual de la Universidad, los recursos faltantes y su alcance para implementar la Firma

[11] Según la planilla Anexa del Art. 3° del Decreto 13/2016 de la República Argentina. Para más información: http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257556/norma.htm

Digital. Por último, se hará un breve resumen detallando los objetivos de la Universidad, los proyectos en donde quiere implementar firma digital, el alcance, un presupuesto estimado y las actividades que debe seguir para adherirse a la Ley Nacional N° 25506.

5.1.1 Autoridad Certificante de la ONTI

Como se explicó en el capítulo anterior, el Certificador o Autoridad Certificante de la Oficina Nacional de Tecnologías de Información (AC-ONTI), con el fin de distribuir el proceso de tramitación de los certificados de firma digital, posee una estructura de Autoridades de Registro (AR) constituidas por entes públicos (ver Figura 10), las que serán responsables de efectuar las funciones de validación de identidad y de otros datos de los solicitantes y suscriptores de certificados digitales, de acuerdo al ámbito de aplicación establecido para cada una de ellas (ONTI, 2015 A, p.4).

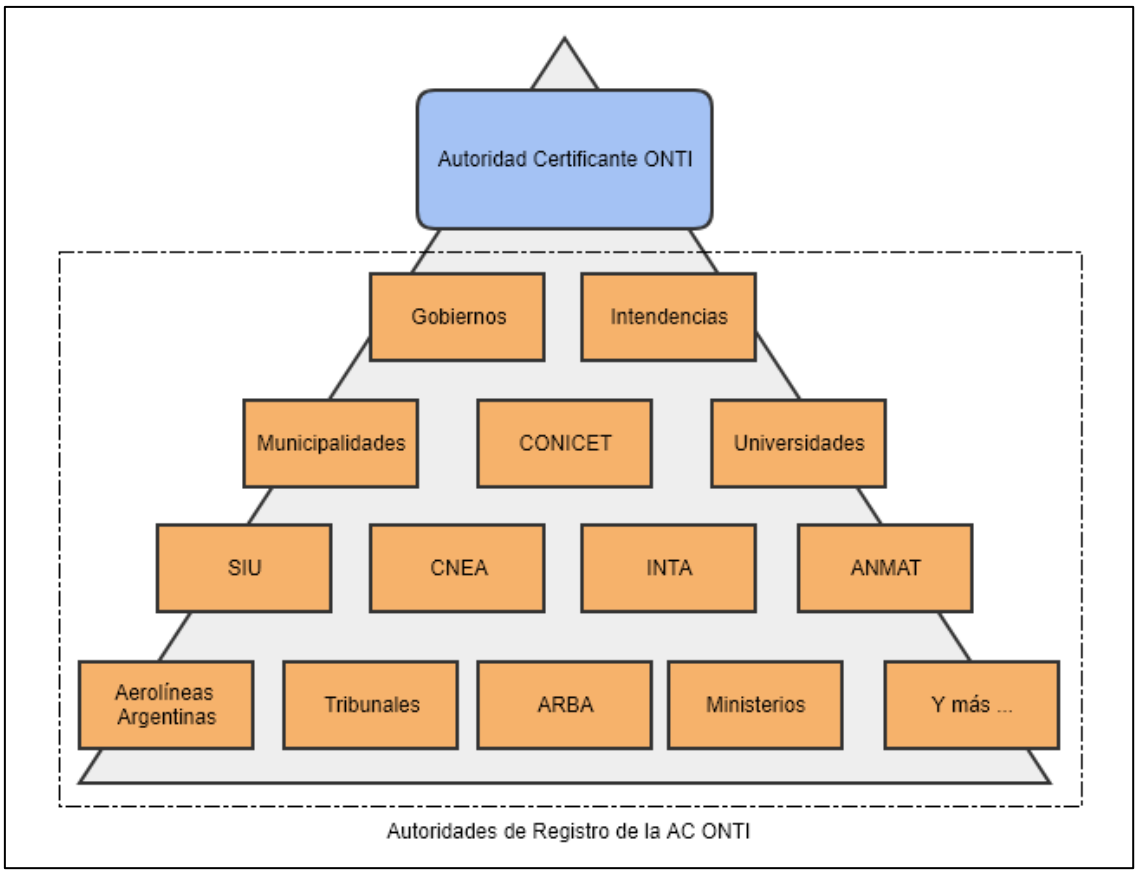


Figura 10: Estructura de Autoridades de Registros

Para determinar el ámbito de aplicación de cada AR es necesario definir:

1. Dominio de correo electrónico del ente público en el que se constituye la Autoridad de Registro: la UNRN se encargará de evaluar las solicitudes de certificados de los empleados o agentes de su jurisdicción para los dominios de correo electrónico “unrn.edu.ar”.
2. Alcance de la aplicación para la cual se constituye la Autoridad de Registro: en el caso de que la UNRN posea una aplicación informática transversal para interactuar con otros entes y requerir el uso de certificados de firma digital, aprobará solicitudes de certificados a empleados o agentes que necesiten disponer de una firma digital para ser utilizada en dicha aplicación informática. La UNRN no dispondrá, en un principio, de una aplicación informática transversal (ONTI, 2015 A, p.6).

5.1.2 Autoridad de Registro

Más específicamente, las AR serán las encargadas de facilitar el proceso de registración de los solicitantes y suscriptores de certificados, para ello deberán efectuar las funciones de aprobación o rechazo de las solicitudes, así como también la de revocación y renovación de los certificados digitales siguiendo las pautas establecidas por la Política de Certificación y el Manual de Procedimientos de Certificación licenciados de la AC-ONTI (ONTI, 2015 A, p.6-7).

Las AR se rigen por una jerarquía estricta que excluye a toda persona ajena a la institución. Por ejemplo, un agente con trabajo en la Universidad no podrá requerir la certificación de la firma digital en la Administración Federal de Ingresos Públicos (AFIP) alegando que trabaja en la Universidad; sin embargo, podrá obtenerla en el Ministerio de Educación, ya que todo establecimiento público educativo depende de él.

5.1.2.1 Obligaciones de una Autoridad de Registro

La UNRN, en su carácter de futura AR (de ahora en más AR-UNRN), deberá cumplir con los siguientes requisitos establecidos por la AC ONTI:

a. Recibir las solicitudes de emisión de certificados.
b. Implementar un nivel de seguridad física (denominado “Nivel 1”) a fin de garantizar su correcto funcionamiento y la protección adecuada de la información y documentación presentada por el solicitante o titular.
c. Informar a la AC-ONTI cualquier cambio del personal perteneciente a la AR.
d. Remitir al Certificador la documentación de respaldo digitalizada a fin de asegurar procedimientos y mecanismos adecuados de recuperación frente a imprevistos que pueden afectar la operatoria de la AR.

e. Verificar que los usuarios que requieran un certificado con nivel de seguridad alto utilicen un dispositivo (llamados tokens) que cumple con el estándar de certificación FIPS 140-2 Nivel 2 o superior Overall.

f. Designar y asegurar la disponibilidad de todos los roles integrantes que conformarán la AR: Responsables de la Autoridad de Registro, Oficiales de Registro y Soporte Técnico de Firma Digital.

g. Instruir y asistir a solicitantes o suscriptores en la tramitación de los servicios provistos por el Certificador, las buenas prácticas y en el manejo de la operatoria de la tecnología de firma digital de las distintas aplicaciones que requieran su uso por medio de la designación de un Soporte Técnico de Firma Digital quién será el responsable encargado de ejercer esa tarea.

h. Cumplir con cualquier otra disposición que establezca la normativa vigente o la AC-ONTI en su calidad de Certificador Licenciado.

i. En caso de realizar la actividad en puestos móviles, será necesario implementar los controles de seguridad que garanticen un proceso confiable de aprobación de solicitudes de emisión, renovación o revocación de certificados.

5.1.2.2 Funciones de la Autoridad de Registro

A partir de lo establecido en la Política Única de Certificación y el Manual de Procedimientos de la AC-ONTI se desprende que la AR-UNRN deberá realizar, entre otras, las siguientes funciones a través de sus Oficiales de Registros habilitados:

a. Exigir la presencia física del solicitante o suscriptor a fin de validar indubitablemente su identidad y la titularidad de su clave pública asociada.

b. Cumplir con los requisitos establecidos (apartado 1.3.3 del Manual de Procedimientos de la ONTI) para la aprobación de solicitudes de certificados de personas físicas o jurídicas que realicen trámites con el Estado.

c. Validar contra la documentación respaldatoria los demás datos de los solicitantes o suscriptores que se van a incluir en el certificado a emitir.

d. Aprobar o rechazar las solicitudes de certificados y remitirlas a la AC-ONTI para su emisión según corresponda.

e. Archivar y conservar toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por la AC-ONTI. Actualmente debe ser almacenada por DOCE (12) años dentro del nivel de seguridad 1 de la AR, requiriéndose asimismo que sea digitalizada, firmada y subida en la aplicación de la AC-ONTI.

f. Proteger su par de claves, de manera que su clave privada se encuentre en todo momento bajo su exclusivo conocimiento y control, en cumplimiento con todas las medidas de seguridad establecidas por el certificador. Para ello los Oficiales de Registro de las AR deberán poseer certificados con nivel de seguridad Alto, o sea que la clave privada y certificado de cada uno debe haber sido tramitado utilizando un dispositivo criptográfico FIPS 140-2 Nivel 2 o superior Overall certificado por el Instituto Nacional de Estándares y Tecnologías o NIST por sus siglas en inglés (National Institute of Standards and Technology).

5.1.2.3 Estructura de la UNRN como AR

El siguiente gráfico muestra la estructura tipo de una AR detallando los roles que se deben contemplar:

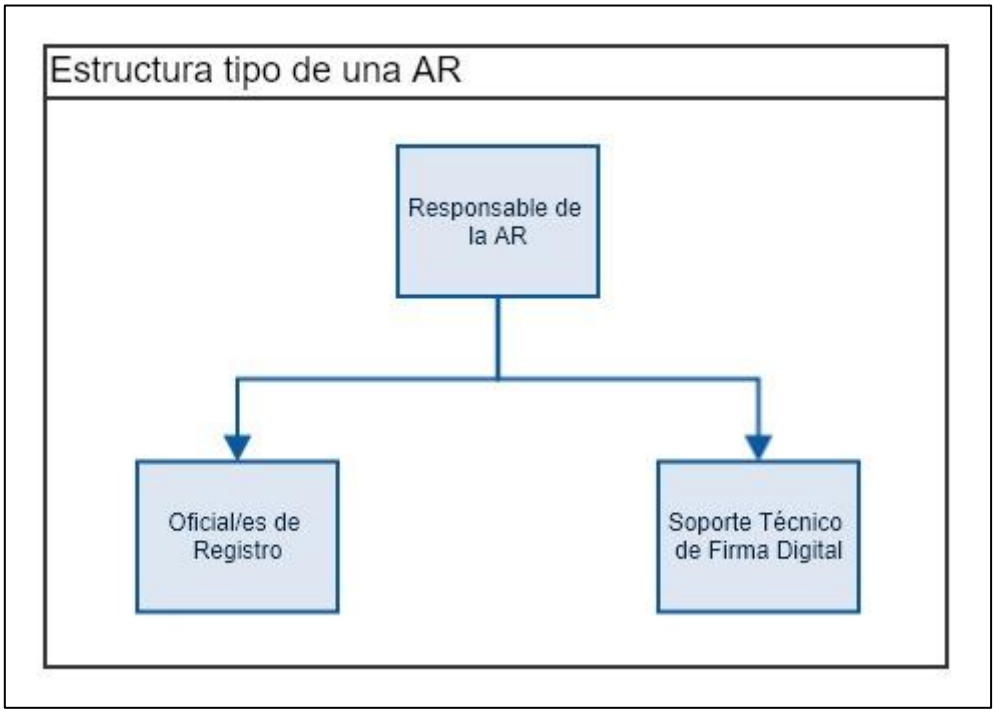


Figura 11: Estructura tipo de una AR

Una Autoridad de registro debe estar conformada por:

- Al menos UN (1) Responsable de Autoridad de Registro, se sugieren TRES (3).
- Al menos DOS (2) Oficiales de Registro, se sugieren TRES (3).
- Al menos UN (1) Soporte Técnico de Firma Digital.

Asimismo, deberá poseer al menos UN (1) domicilio postal declarado al Certificador donde se constituirá el Nivel 1 en el cual atenderán y operarán los Oficiales de Registro.

La cantidad de personas a designar en cada rol y los domicilios postales a declarar deberá ser evaluada por la Universidad en función de la demanda que ésta prevea, debiendo respetarse el número mínimo señalado anteriormente (ONTI, 2015 A, p.11).

A continuación, se detallan las funciones principales de cada rol:

Responsable de la Autoridad de Registro

- Son los nexos formales de comunicación entre el Responsable de la AC-ONTI y la Autoridad de Registro.
- Designan a quienes desempeñarán los roles dentro de la Autoridad de Registro (Oficiales de Registro y Soporte Técnico de Firma Digital).
- Controlan el cumplimiento de la Política Única de Certificación de la AC ONTI.
- Mantienen informado al Certificador sobre cualquier modificación en la conformación de la AR: designación o desvinculación de Oficiales de Registro, Soporte Técnico de Firma Digital, alta y baja de dominios asociados a la AR, domicilio físico donde se encuentre constituida la AR y sobre las aplicaciones que utilicen los certificados de la AC ONTI (ONTI, 2015 B, p.7).

Oficial de Registro

- Son los responsables de ejecutar la operatoria principal de la AR, así como también de cumplir con las obligaciones, funciones y recaudos de seguridad que la AC-ONTI le delega.
- Aprueban solicitudes de certificados de firma digital a partir de la validación de la identidad del solicitante, de la titularidad de su clave pública y de los demás datos de la solicitud según las pautas establecidas por la Política Única de Certificación y por el Manual de Procedimientos de la AC-ONTI.
- Rechazan solicitudes de certificados que no cumplen con los requisitos establecidos en la Política y Manual de Procedimientos anteriormente mencionados.
- Revocan certificados siguiendo las pautas de la Política y Manual de Procedimientos anteriormente mencionados.

Es requisito, para ejercer este rol, poseer un certificado de firma digital de nivel de seguridad alto, válido y vigente emitido por el sistema. Esto implica que su

clave privada deberá permanecer guardada en un dispositivo criptográfico, homologado por el Certificador y que cumpla con la normativa FIPS 140 nivel 2 (ONTI, 2015 B, p.7-8).

Soporte Técnico de Firma Digital

- Instruir acerca de las buenas prácticas de utilización de la tecnología de firma digital y de su marco legal expresada en la Política de Certificación Licenciada de la ONTI.
- Identificar y reconocer los dispositivos criptográficos que cumplan con la certificación de NIST FIPS 140-2 Nivel 2 o superior que requieren los solicitantes de certificados de nivel de seguridad alto.
- Difundir la tecnología de firma digital en su organismo a fin de que los agentes de esa jurisdicción tomen conocimiento de la posibilidad de acceso a la tecnología de firma digital a través de la AR constituida.
- Asistir a los solicitantes o suscriptores en ámbito de su AR en en el proceso de tramitación de los servicios provistos por el Certificador y en el manejo de la operatoria de la tecnología de firma digital de las distintas aplicaciones que requieran su uso (ONTI, 2015 B, p.8).

Teniendo en cuenta lo mencionado anteriormente, la figura 12 plantea una posible estructura que puede implementar la UNRN cómo AR, detallando los roles y los departamentos involucrados.

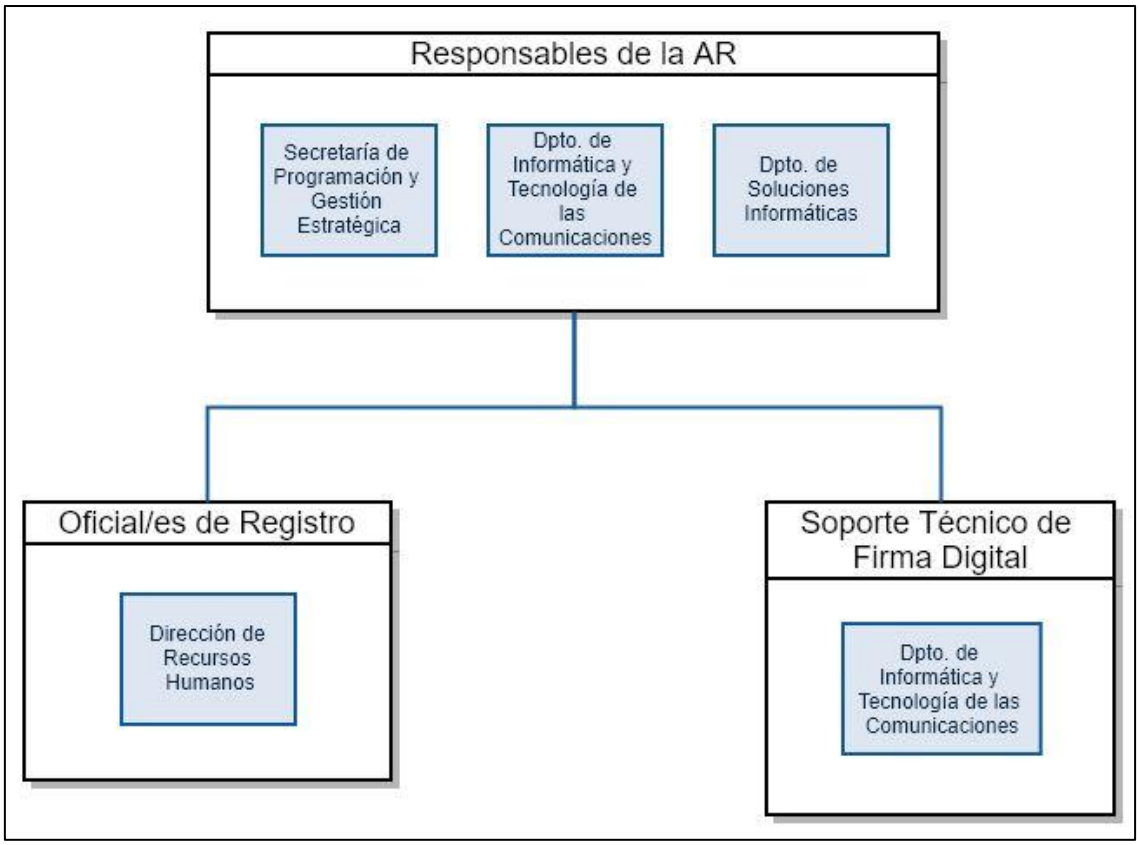


Figura 12: Designación de roles de la AR-UNRN

5.1.2.3.1 Organización de la UNRN

5.1.2.3.1.1 Por Oficinas de Registro

Además, según el art. 36° del Decreto 2628 del año 2002, una Autoridad de Registro puede constituirse como una única unidad o con varias unidades dependientes jerárquicamente entre sí, pudiendo, delegar su operatoria en otras autoridades de registro, siempre que medie la aprobación del Certificador Licenciado, en este caso la ONTI (Decreto 2628, 2002, Art. 36°). Si bien, no es necesario que la UNRN cree una AR en cada Sede, puede ser conveniente la conformación de una Oficina de Registro por Sede. La figura 13 muestra la estructura jerárquica de la AR que conformaría la Universidad.

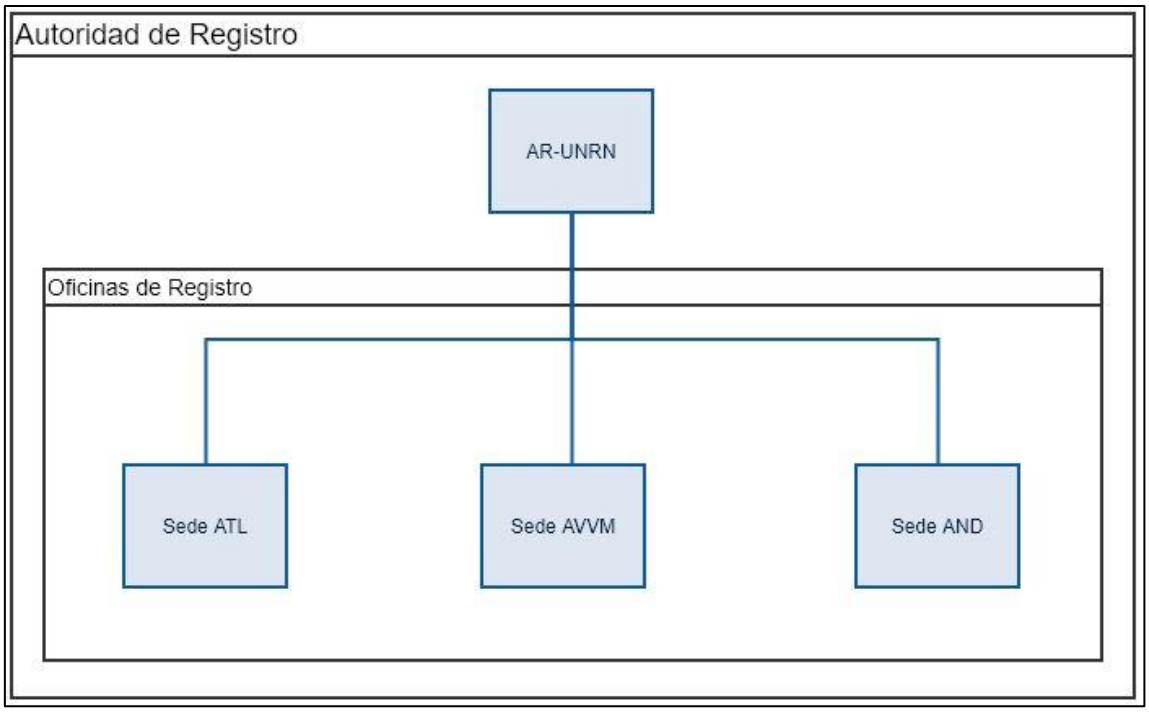


Figura 13: Estructura de AR-UNRN con Oficina de Registro fija

Una vez constituida la AR, el Rectorado, perteneciente a la Región Atlántica, se conformará como la primer Oficina de Registro de la Universidad. Por lo tanto, esta implementación progresiva espera contar con una oficina en cada sede con el objetivo de reducir la brecha geográfica.

5.1.2.3.1.2 Por Modalidad Móvil

Por otro lado, se puede optar por la incorporación de la modalidad móvil. Es decir, una vez constituida por lo menos una Oficina de Registro se procederá a habilitar la modalidad móvil teniendo en cuenta las especificaciones descritas en el apartado 5.1.2.7.3. De esta manera, la AR-UNRN deberá asignar a un Oficial de Registro que opere fuera de su domicilio previamente declarado cuando así se requiera, tal como se muestra en la figura 14.

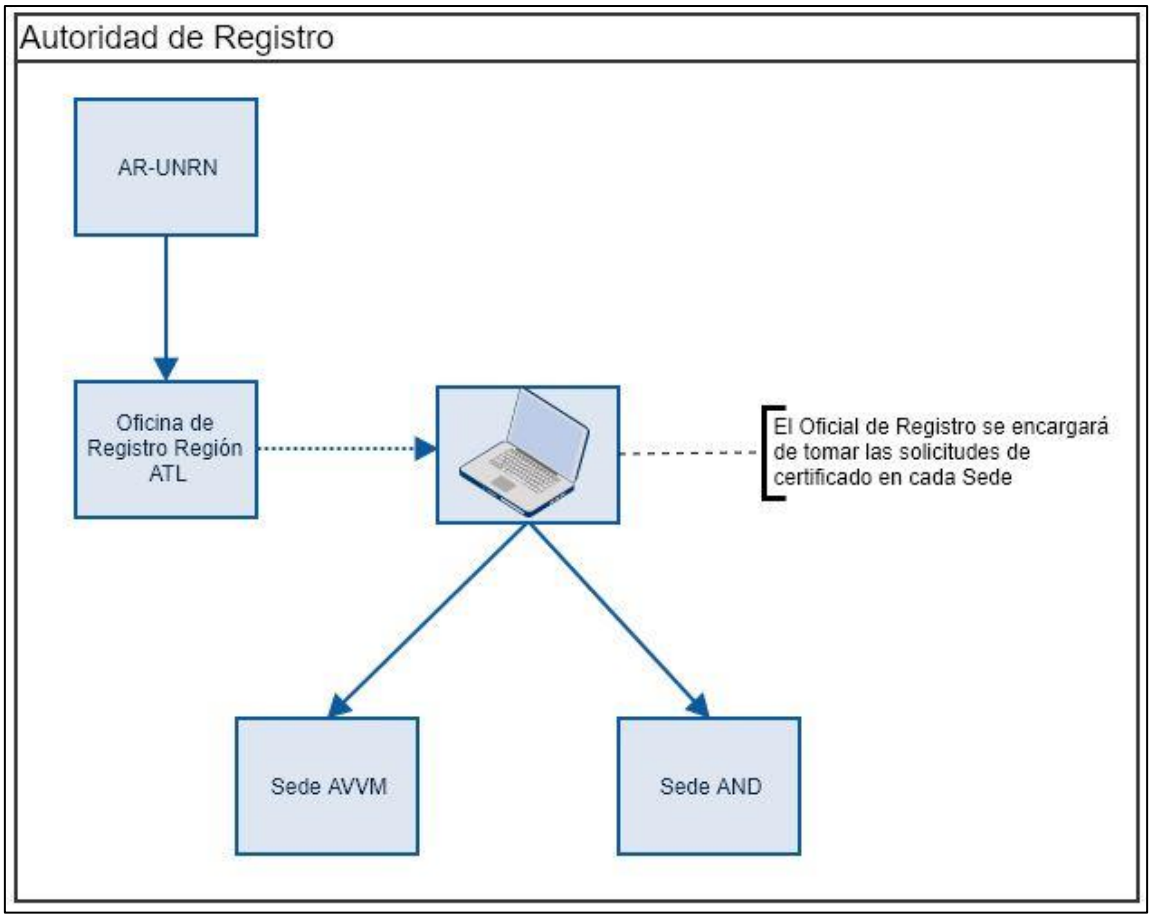


Figura 14: Estructura de AR-UNRN con Oficina de Registro móvil

La modalidad móvil es un anexo a la modalidad fija. Es decir, que los organismos que quieran conformarse como AR deberán informar a la AC ONTI si, adicionalmente, optarán por funcionar en puesto móvil, no pudiendo desarrollar su actividad exclusivamente en dicha modalidad (ONTI, 2015 B).

5.1.2.4 Requerimientos normativos para la conformación de AR.

Conforme surge de los términos del Decreto Reglamentario N° 2628/02, el art. 39° menciona que, en las entidades y jurisdicciones pertenecientes a la Administración Pública Nacional, las áreas de recursos humanos deben cumplir las funciones de Autoridades de Registro para los agentes y funcionarios de su jurisdicción. En el caso, y si las aplicaciones de que se trate lo requieren, la máxima autoridad del organismo podrá asignar, adicionalmente, a otra unidad las funciones de Autoridad de Registro.

Partiendo del análisis anterior y siguiendo con los términos de la Política Única de Certificación y con el Manual de Procedimientos de la AC-ONTI, la estructura de la Autoridad de Registro de la Universidad Nacional de Río Negro deberá conformarse en el Área de Recursos Humanos o equivalente. En ese sentido, al menos UN (1) Oficial de Registro deberá reportar a dicha área. En caso de que

la Universidad requiera conformar otra Autoridad de Registro adicional a la de Recursos Humanos deberá solicitar al certificador la correspondiente autorización.

El AC-ONTI procederá a aprobar o bien a denegar la solicitud de autorización, haciéndole saber al Organismo respecto de las obligaciones y responsabilidades que asume al respecto, conforme lo determina el artículo 36 del Decreto Reglamentario N° 2628/02 (ONTI, 2015 A, p.14).

5.1.2.5 Procedimiento de conformación de la Autoridad de Registro

Para iniciar los trámites de la conformación de una AR, la Universidad deberá seguir los siguientes pasos:

Paso 1: Presentación de documentación para la constituir la Autoridad de Registro.

A fin de conformar la AR, la Universidad Nacional de Río Negro deberá presentar las siguientes notas ante la AC-ONTI:

1) Nota firmada por la máxima autoridad, el Rector, solicitando autorización para conformar la AR, asistencia para su implementación y designando los Responsables de la AR (al menos UN (1), pero se sugieren TRES (3)). En la misma nota se deberá informar las aplicaciones o proyectos en los que prevé el uso de la firma digital. Por lo menos un Responsable de la AR deberá formar parte del Dpto. de Recursos Humanos.
2) Nota firmada por el o los Responsables de la AR informando:
    a. La designación de los Oficiales de Registro (al menos DOS (2), se sugieren como mínimo TRES (3)) y de Soporte Técnico de Firma Digital (al menos UN (1)) detallando:
        i. Tipo y número de documento de identidad.
        ii. Cuenta de correo electrónico institucional (cuyo dominio tiene que ser unrn.edu.ar)
        iii. Teléfono de contacto institucional (incluyendo internos)
    b. El o los dominios de correo electrónico de la futura AR (ej: ar@unrn.edu.ar, firma.digital@unrn.edu.ar, pki@unrn.edu.ar o autoridad.registro@unrn.edu.ar, entre otras) para asignar a la aplicación de la AC-ONTI.
    c. Domicilios postales declarando los lugares físicos donde operan los Oficiales de Registro. Por ejemplo, “Belgrano 526 - Piso 1 - Oficina A - Departamento de RRHH”.

3) En caso de adoptarse la modalidad de Autoridad de Registro móvil, deberá presentarse además la solicitud de autorización para funcionar en dicha modalidad firmada por la máxima autoridad del organismo (ONTI, 2015 A).

Las notas serán provistas por la AC ONTI, previo envío de correo electrónico informando la intención de conformar una AR. Sin más, ambas notas se encuentran en el Anexo A de este documento.

Paso 2: Curso de capacitación para el personal de la AR.

Una vez aprobada la documentación presentada, los agentes designados en los distintos roles de la AR-UNRN deberán concurrir a la ONTI, específicamente al Laboratorio de Firma Digital, a fin de recibir un curso de capacitación de carácter obligatorio.

Los postulantes a Oficiales de Registro deberán aprobar el examen referido al curso mencionado, el cual se envía por correo electrónico teniendo un plazo aproximado de DIEZ (10) días para remitir las respuestas. En caso de no aprobar el examen, el OR reprobado tendrá una nueva oportunidad para rendirlo, y si vuelve a reprobarlo, deberá realizar nuevamente el curso de capacitación.

A través de la capacitación, los futuros Oficiales de Registro de la UNRN aprenderán, de una forma sencilla, las políticas y procedimientos que forman parte de la gestión del Certificador AC-ONTI. A su vez, permitirá al Soporte Técnico de Firma Digital conocer sus responsabilidades y funciones para la correcta asistencia a los solicitantes de certificados que interactuarán con la UNRN. El curso, de dos días de duración, ofrece información tanto teórica como práctica sobre el uso de esta herramienta, y la oportunidad de experimentar, en un ambiente de prueba, la gestión y emisión de un certificado y su utilización en el correo electrónico.

Paso 3: Tramitación de certificados de Oficiales de Registro

Los Oficiales de Registro que aprueben el examen deberán efectuar el trámite de solicitud de sus certificados digitales ante la AC-ONTI, para lo que deberán concurrir personalmente con la documentación de respaldo (Documento de identidad, constancia de CUIL / CUIT, certificado de cargo) y dispositivo criptográfico FIPS 140-2 Nivel 2 o superior. La tramitación de los certificados de los Oficiales de Registro podrá demorarse de dos a tres semanas.

Paso 4: Habilitación de la Autoridad de Registro

Efectuada la aprobación de los exámenes y emitidos los certificados de los Oficiales de Registro, se procederá a habilitar a la UNRN como AR, y a enrolar a los mencionados Oficiales de Registro en la aplicación de la AC-ONTI. A partir

de ese momento, que puede ser de una a dos semanas, podrán comenzar a operar en su función (ONTI, 2015 A, p.15-17).

5.1.2.6 Modificación de roles designados o demás cargos de la AR

En caso de que haya nuevas designaciones o se produzca la desvinculación de alguno de los roles involucrados en la AR (Oficial de Registro o Soporte Técnico de Firma Digital), dicha situación deberá ser informada por el Responsable de la AR por medio de nota formal o por correo electrónico firmado digitalmente dirigido al Responsable de la AC-ONTI. En caso de producirse alguna modificación en el rol de Responsable de la AR, la novedad deberá ser informada por la máxima autoridad del organismo por los mismos medios (ONTI, 2015 A, p.17).

5.1.2.7 Requerimientos a cumplir por las instalaciones de las Autoridades de Registro

5.1.2.7.1 Seguridad Física

La seguridad física consiste en aplicar barreras y procedimientos de control con el objetivo de tomar medidas de prevención ante amenazas (ver Figura 15) a los recursos e información confidencial que se encuentren dentro del Nivel 1 de seguridad. No sólo se debe controlar la seguridad del hardware y medios de almacenamiento de datos dentro y fuera del Nivel 1, sino también los medios de acceso remoto al y desde el mismo (Litwak & Escalante, 2004, p.21).

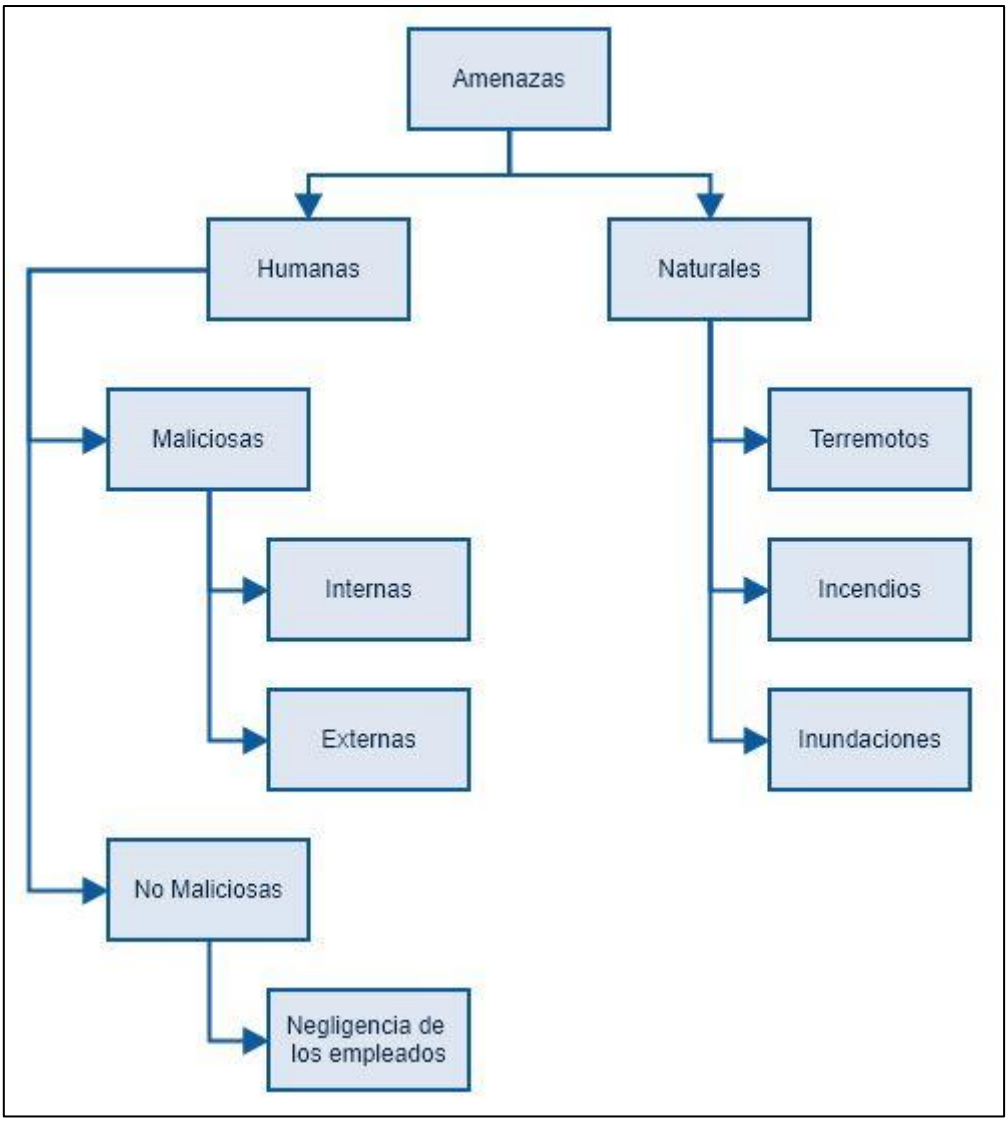


Figura 15: Tipo de amenazas

Por lo tanto, la AR-UNRN debe implementar un sistema de seguridad física que garantice su correcto funcionamiento y la protección adecuada de la información y documentación presentada por el solicitante o titular del certificado digital. En este sentido, deberán extremarse las medidas que impidan el acceso no autorizado al puesto de trabajo de la AR y a la documentación que se le confía para su resguardo, así como a los datos de los solicitantes. Asimismo, deberá contar con adecuados procedimientos y mecanismos de recuperación frente a eventos imprevistos.

La AR-UNRN podrá realizar su actividad en puestos móviles cuando se presenten las condiciones que ameriten tal servicio, siempre que lo haya aprobado el ente licenciante y no se vulneren los controles de seguridad que garanticen un proceso confiable de aprobación de solicitudes de emisión, renovación o revocación de certificados (ONTI, 2015 A).

5.1.2.7.2 Operaciones de las Autoridades de Registro Fija

5.1.2.7.2.1 Requerimientos

La AR-UNRN debe funcionar dentro de un nivel físico de seguridad, denominado anteriormente como Nivel 1. Este será el mínimo nivel de seguridad requerido para la realización de cualquier operación de la AR; en consecuencia, los Oficiales de Registro deben efectuar todas las operaciones relativas a su función dentro de este nivel de acceso.

Las instalaciones donde residirá la AR deberán contar con matafuegos autorizados y además, en caso de alguna eventualidad, debe permitirse la evacuación segura de las personas que hayan ingresado a dicho nivel de acceso (ONTI, 2015 A, p.18).

Por lo tanto, la Oficina de Registro de la AR-UNRN deberá estar instalada en un ambiente dedicado y contener lo siguiente:

- Equipo de prevención de incendios: Detectores de Humo y matafuegos HCFC 123 (son agentes limpios y no dejan residuos luego de la extinción).
- Material refractario resistente al fuego y gases corrosivos.
- Archivador ignífugo[12] con llave y de uso exclusivo de los responsables de la AR.
- Tensión estabilizada.
- Equipamiento informático protegido por Sistema de alimentación ininterrumpida o UPS (Uninterruptible Power Supply, por sus siglas en inglés).
- Cables ordenados y protegidos dentro de ductos adecuados.
- Única puerta de entrada/salida hermética, con cerradura adecuada y acceso con tarjeta inteligente u algún dispositivo biométrico)
- Paredes y techo adecuados para impedir el acceso no autorizado.
- En caso de que el ambiente posea ventanas u otras aberturas hacia el exterior, éstas deben impedir la visibilidad y el acceso externo.
- Iluminación de emergencia.
- Filtrado de Aire y Humedad (Aire Acondicionado)
- Limpieza y mantenimiento permanente.
- Cámaras de seguridad conectadas vía IP.
- Computadora conectada a internet, preferentemente no a la red del establecimiento.

[12] Según la RAE, la palabra ignífugo hace referencia a la propiedad o característica de un elemento o material para que no se inflame ni propague la llama o el fuego.

- Impresora conectada directamente a la PC.

La figura 16 muestra un bosquejo de cómo debería estructurarse el Nivel 1 dentro de la AR-UNRN.

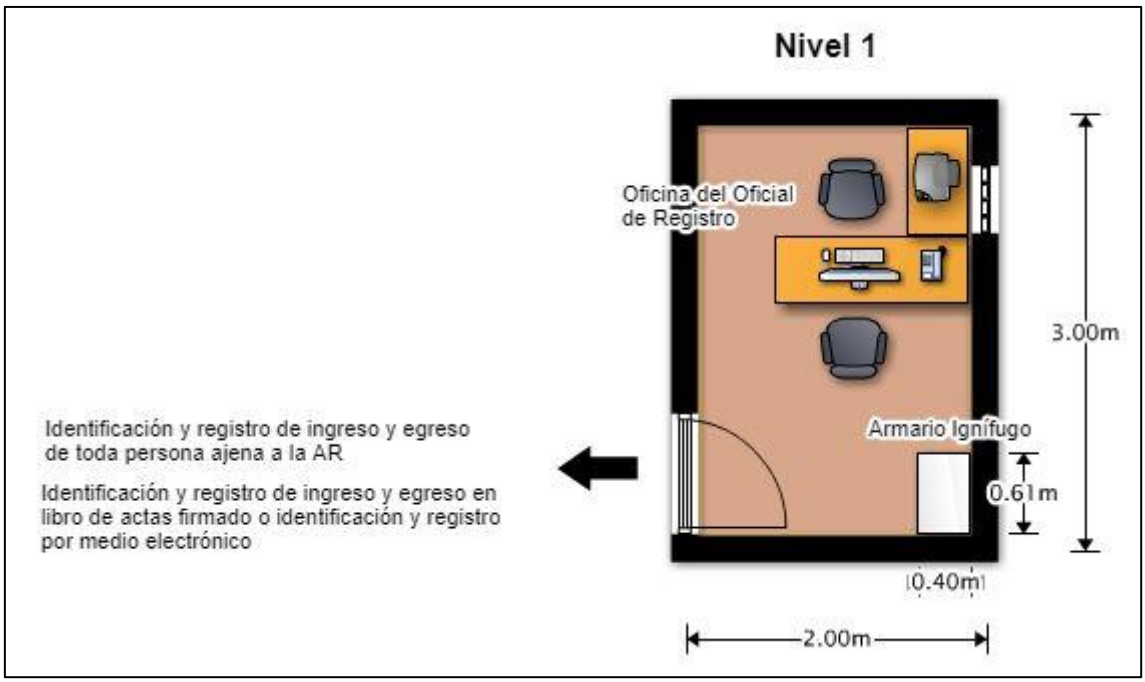


Figura 16: Seguridad del Nivel 1

5.1.2.7.2.2 Declaración del Nivel 1

El domicilio postal donde se encuentra dicho Nivel 1 debe ser declarado por nota formal del Responsable de la AR, no pudiendo éste operar en otro lugar físico con domicilio postal que no esté previamente declarado.

Por ejemplo, en la UNRN, en su carácter de futura Autoridad de Registro de la ONTI, podría tener como domicilio postal declarado Belgrano 526 - Piso 1 - Oficina A - Departamento de RRHH.

Un Oficial de Registro no deberá operar en otro lugar físico que no sea aquel o aquellos domicilios postales declarados, exceptuando el caso de que la AR-UNRN opere bajo modalidad móvil (ONTI, 2015 A).

5.1.2.7.2.3 Registro

Para al acceso al Nivel 1 se deberá registrar el ingreso y egreso a los puestos de atención constituidos de quienes acceden para realizar sus trámites relacionados con la gestión de sus certificados. La identificación deberá realizarse mediante la presentación del documento de identidad del ingresante. El registro de ingreso y egreso se realiza en el libro de actas donde se registre:

fecha y hora, número de serie o secuencia del registro, apellido, nombre, tipo y número de documento, organismo o empresa si corresponde, motivo de ingreso y firma hológrafa del ingresante o del que egresa; además firma del Oficial de Registro que efectúa dicho registro.

Los libros de actas de una AR deben estar identificados con números de serie consecutivos y con el domicilio postal al que pertenecen, comenzando por el UNO (1). Deben tener la leyenda “Registro de Ingresos y Egresos Nro. XX”, donde XX significa el número de serie identificatorio asignado a ese registro (ONTI, 2015 A, p.20).

Para el ingreso al Nivel 1 se podrá implementar la utilización de un sistema de acceso controlado mediante el uso de tarjetas de banda magnética. Inventadas en la década del 60, estas tarjetas pueden almacenar información, automatizar los procesos, proveer una lectura rápida y fácil de la información, incrementar la productividad y eliminar el error humano, en el caso de utilizar otro método de acceso como la entrada por código. La tecnología de banda magnética es económica y durable, ya que una tarjeta puede ser desechada y reutilizada.

En este caso, el Oficial de Registro, además de registrar el egreso junto con el solicitante, le entregará una tarjeta numerada, que también deberá registrarse en el acta. La información contenida en la tarjeta de banda magnética pasará por un lector, dispositivo electrónico que actúa como interfaz entre el usuario y el sistema, para ser procesada con el fin de autenticar o no el ingreso al Nivel 1. Una vez realizado el trámite correspondiente, tanto el Oficial de Registro como el solicitante deberán registrar la salida indicando la tarjeta utilizada.

5.1.2.7.2.4 Resguardo de documentación

Toda la documentación de respaldo en papel de los procesos de aprobación, revocación y rechazo, tanto en modalidad fija como móvil, así como el registro de ingresos y egresos al Nivel 1, debe ser resguardada dentro de este nivel en un armario cuyo acceso debe estar restringido únicamente a los Oficiales de Registro y a los Responsables de la AR.

Dicha documentación deberá ser resguardada por un período de DIEZ (10) años a partir del vencimiento o revocación del certificado o del rechazo de la solicitud. Adicionalmente deberá resguardarse la documentación establecida en el apartado “Controles de Gestión de las AR”. La documentación resguardada sólo podrá abandonar el Nivel 1 en caso de que la Oficina de Registro deba ser mudada (ONTI, 2015 A, p.24).

5.1.2.7.3 Operaciones de las Autoridades de Registro Móvil

5.1.2.7.3.1 Requerimientos

Según el Manual de Procedimientos, todas las AR que estén habilitadas para operar adicionalmente en la modalidad de puesto móvil deben cumplir con los siguientes requisitos de seguridad, para la operación de sus ORs:

- Realizar el proceso de aprobación de solicitudes en recintos donde no haya personal ajeno al proceso, cerciorándose de que no existan cámaras, dispositivos de captura de imágenes o aberturas que permitan la visualización externa del proceso de aprobación y generación de claves, ni otros datos de creación de firma digital.
- Utilizar equipamiento propio de la AR (PC o Notebook), que garantice la seguridad de la información, similares a las utilizadas en las instalaciones fijas (sistema operativo y antivirus actualizados y con soporte, así como otras configuraciones de seguridad aplicables).
- Realizar el resguardo digital de la documentación de respaldo, preferentemente en el momento en que se aprueba la solicitud, utilizando un dispositivo propio o de la instalación donde se realiza el proceso de aprobación; firmarla digitalmente y cargarla en la aplicación de la AC-ONTI.
- Garantizar que la documentación de respaldo se encuentra bajo su control desde el momento en que la recibe hasta su resguardo en las instalaciones del organismo en la que funciona la AR (ONTI, 2015 B, p.10).
- Los procedimientos de los ORs en las actividades relativas a la autenticación de la identidad de solicitantes y procesamiento de las solicitudes son idénticos a los realizados en las instalaciones fijas de la AR (ONTI, 2015 A, p.23).

Un OR vinculado a una AR, que fue autorizada a funcionar en puesto móvil, podrá operar fuera de su domicilio habitual declarado cuando las circunstancias lo requieran. Una AR autorizada a funcionar en modalidad móvil no podrá tener ORs operando en esta modalidad en un lugar físico permanente no declarado.

5.1.2.7.3.2 Registro

El OR que va a operar en puesto móvil deberá, previamente, dejar asentado su salida en el libro de actas de ingresos y egresos del domicilio postal donde opera, indicando fecha y hora de salida y motivo del trámite.

Durante el proceso de operación, el OR interviniente deberá registrar en un acta volante las operaciones en modalidad móvil, indicando los mismos datos que acta fija. Estas actas volantes deben estar identificadas con números de serie consecutivos, comenzando por el UNO (1) e independientes de los utilizados

para identificar los libros de actas de la AR fija o los registros de ingresos y egresos.

Cuando regrese a la Oficina de Registro fija, el OR que operó en puesto móvil, deberá registrar su regreso, con fecha y hora, e indicar los números de serie de las actas volantes confeccionadas y cualquier otra novedad que pudiera ser de interés para la operatoria de la AR (ONTI, 2015 A, p.24).

5.1.2.7.3.3 Resguardo de la documentación

Culminada la operatoria del OR en su modalidad de puesto móvil, toda documentación de respaldo en papel de los procesos de aprobación, revocación y rechazo, incluyendo las actas volantes, debe ser resguardada dentro del Nivel 1; de igual forma debe ser referenciada el acta volante en el libro de actas correspondiente.

5.1.2.7.4 Seguridad Lógica.

La seguridad lógica consiste en la aplicación de procedimientos y técnicas empleadas para proteger los datos, procesos y programas, así como también el acceso ordenado y autorizado de los usuarios a los sistemas de información.

Los aspectos de seguridad lógica a tener en cuenta en las instalaciones de la AR-UNRN comprenden como mínimo que el equipamiento se encuentre protegido contra amenazas y acciones no autorizadas, tanto para el acceso como para el uso de los equipos informáticos y la información relacionada con las operaciones. Se deberá tener en cuenta al menos las siguientes configuraciones de seguridad:

a. Clave de acceso al equipo.
b. Exigencia de uso de contraseñas robustas (8 caracteres, incluidas mayúsculas y números).
c. Para la utilización del Sistema Operativo Windows 7 o superior, los antivirus, anti-troyanos y antispyware deberán estar activados y actualizados.
d. El firewall de la estación de trabajo debe estar activado, con los permisos de accesos mínimos necesarios para efectuar las actividades, pudiendo ser sustituido por un firewall corporativo (si lo requiere), para los equipamientos conectados en redes.
e. El protector de pantalla debe encontrarse activado y bloquearse, a lo sumo, luego de DOS (2) minutos de inactividad, exigiendo contraseña para el desbloqueo.

f. El sistema operativo y la totalidad de las aplicaciones instaladas en la estación de trabajo deberán mantenerse actualizados (parches, hotfix, etc.) (ONTI, 2015 A, p.24).

Los requerimientos mínimos que debe cumplir una computadora que se ubica en una Oficina de Registro deberían ser:

- SO: Windows 7 o Superior
- Procesador: 2 Gigahercios (GHz) o superior.
- Memoria: 4 Gigabyte (GB) de memoria RAM
- DirectX: Versión 9.0c o superior.
- Gráficos: Compatible DirectX 9 con WDDM 1.0 (Windows Display Driver Model[13]).
- Red: Conexión de banda ancha a Internet
- Almacenamiento: 120 GB de espacio en disco
- Tarjeta de sonido: DirectX Compatible (opcional).

5.1.2.7.5 Controles de Gestión de las ARs

A continuación, se enumeran las carpetas que debe mantener la AR-UNRN y sus contenidos mínimos; toda la documentación detallada debe ser resguardada dentro del Nivel 1.

Carpeta de la instalación técnica de la AR

Reúne el conjunto de documentos relacionados con la instalación técnica, con información actualizada, conteniendo como mínimo:

1. Lista de Oficiales de Registro que estén actuando o hayan actuado en la Autoridad de Registro, con los respectivos números de serie de sus certificados digitales.
2. Autorización del Certificador Licenciado para la conformación de la AR.
3. Listado actualizado con la identificación de todos los libros de actas de registro de ingresos y egresos utilizados.
4. Documentación firmada por el Responsable de la AR donde se encuentren identificados los equipos donde operan los Oficiales de

[13] WDDM es la arquitectura de controladores gráficos para las tarjetas de vídeo de Microsoft a partir de la versión de Windows Vista.

Registro. Cualquier otra característica adicional a registrar debe ser incluida con dicha documentación.

Carpeta del Oficial de Registro

Comprende el conjunto de documentos relacionados con el Oficial de Registro, conteniendo la siguiente información actualizada:

1. Copia de su contrato de trabajo o copia de las páginas de su legajo personal, donde consten su registro de contratación, las condiciones de empleo o comprobante de situación funcional.
2. Declaración donde afirma conocer las funciones que asume y se obliga a cumplir con la política de seguridad del certificador licenciado en sus aspectos pertinentes y las políticas y normas aplicables al Certificador. En esa declaración se debe comprometer a mantener la confidencialidad y la exclusividad de la propiedad de la información y procesos puestos a su disposición por el certificador licenciado y la AR, aun cuando se haya desvinculado.
3. Copia de la designación por parte del Responsable de la AR y constancia de aprobación del curso.
4. Confirmación del certificador licenciado respecto de la inclusión del Oficial de Registro en su sistema de certificación.

Documentación de Operaciones

Reúne el conjunto de las copias de documentos utilizados como respaldo de los procesos de aprobación o rechazo de las solicitudes de emisión del certificado y de las solicitudes de revocación. Dado que cada solicitud de aprobación o rechazo y revocación de certificados debe ser ingresada por Mesa de Entrada del organismo, generando un número de expediente, es obligatorio contar con TRES (3) carpetas:

a. *Carpeta Antecedentes*: Contendrá los expedientes con la documentación de las solicitudes no aprobadas.
b. *Carpeta Solicitudes Aprobadas*: Contendrá los expedientes con la documentación de las solicitudes aprobadas.
c. *Carpeta de Certificados Revocados*: contendrá los expedientes con la documentación de los certificados revocados.

Toda la documentación deberá resguardarse por un periodo de DIEZ (10) años a partir del vencimiento o revocación del certificado o del rechazo de la solicitud. El archivador ignífugo, mencionado en el apartado 5.1.2.7.2.1 “Requerimientos” se utilizará para almacenar dicha información (ONTI, 2015 A, p.25-27).

5.1.3 Verificación de Dispositivos Criptográficos (Token) bajo el estándar FIPS 140-2 Nivel 2 ó Superior.

Las siguientes pautas y lineamientos tienen por objeto orientar a quien cumpla el rol de Soporte Técnico de Firma Digital, dentro de la UNRN, en la validación de las condiciones de los dispositivos criptográficos de acuerdo a los requerimientos de que dispone la Política Única de Certificación de la ONTI (ONTI, 2015 A, p.27).

La Política de Certificación y el Manual de Procedimientos de la AC-ONTI establecen DOS (2) clases de certificados:

1. Certificados con nivel de seguridad **ALTO**: para los certificados solicitados mediante el uso de dispositivos criptográficos como, por ejemplo: tokens, smartcards, etc. Esta característica permite usar el certificado desde cualquier computadora que tenga instalado el driver del dispositivo criptográfico.
2. Certificados con nivel de seguridad **NORMAL**: correspondiente a los certificados solicitados y almacenados vía software como por ejemplo navegadores web (Internet Explorer, Mozilla Firefox, entre otros). Esta característica define que la persona deberá usar su certificado desde la computadora donde creó su clave privada (ONTI, 2015 A, p.30).

5.1.3.1 Destinatarios

Como se mencionó anteriormente, este procedimiento está destinado principalmente a quienes van a cumplir el rol de Soporte Técnico de Firma Digital, a fin de asistir en la verificación de los dispositivos criptográficos de los solicitantes de certificados digitales que hayan optado por un nivel de seguridad ALTO.

La utilización de dicho nivel requiere que el certificado digital generado sea almacenado en dispositivos FIPS 140-2 Nivel 2 o superior, siempre y cuando la marca y modelo de dicho dispositivo haya sido certificado por NIST (ONTI, 2015 A, p.30).

5.1.3.2 Requisitos previos

1. Contar con un dispositivo criptográfico, sobre el cual se realizan todas las verificaciones.
2. Tener a mano el número de certificado emitido por el NIST para el dispositivo criptográfico, el cuál detalla marca y modelo del mismo.
3. Una computadora con acceso a Internet y con al menos un puerto USB habilitado, a fin de poder conectar e interactuar con el dispositivo criptográfico a verificar.

4. Tener instalado en la computadora el driver del correspondiente dispositivo criptográfico; el software de instalación del driver debe ser entregado por el proveedor del dispositivo criptográfico (ONTI, 2015 A, p.30).

5.1.3.3 Procedimiento de verificación del dispositivo criptográfico

El Departamento de Informática y Tecnología de las Comunicaciones de la UNRN adquirió, por medio del departamento de compras, 20 unidades de dispositivos criptográficos de marca y modelo “eToken 5100”. Dicho dispositivo, provisto por la empresa SafeNet, es un token USB de doble factor de autenticación que utiliza tecnología basada en certificados para generar y almacenar credenciales tales como claves privadas, contraseñas y certificados digitales. Para autenticarse, los usuarios deben proporcionar tanto su autenticador personal SafeNet como su contraseña, proporcionando un segundo nivel de seguridad crítico, más allá de las contraseñas simples para proteger valiosos recursos empresariales digitales.

La verificación de los dispositivos criptográficos se puede realizar accediendo al listado de certificaciones publicados por el NIST a través del siguiente link:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search

En la página web, NIST proporciona, por medio de un buscador, acceso a la información de validación oficial de todos los módulos criptográficos que se han probado y validado bajo el Programa de Validación de Módulos Criptográficos (CMVP por sus siglas en inglés) como requisitos de FIPS 140-1 y FIPS 140- 2. Los resultados de búsqueda enumeran todos los certificados de validación emitidos que cumplen con los criterios de búsqueda provistos y proporcionan un enlace para ver información más detallada sobre cada certificado. La lista del certificado proporciona la información detallada del módulo, incluidas referencias de implementación de algoritmo para la validación del algoritmo CAVP[14], políticas de seguridad, imágenes de certificados originales o referencias a las listas de validación consolidadas, y enlaces de productos de proveedores, si se proporcionan (Validated Modules, 2016).

En el sitio, se encuentran listados los productos que han recibido su certificación de la siguiente manera:

Certificate Number	Vendor Name	Module Name	Module Type	Validation Date	Status

[14] El Programa de Validación de Algoritmos Criptográficos (CAVP) proporciona pruebas de validación de algoritmos criptográficos aprobados por NIPS y recomendados por FIPS y sus componentes individuales.

- Certificate Number: Indica el número de certificado otorgado por NIST.
- Vendor Name: Indica la empresa u organización que realizó el trámite de certificación para un producto determinado.
- Module Name: Módulo criptográfico que recibe la certificación. En esta columna se indica el nombre del producto, identificándose marca, model, versión del hardware y firmware, así como otros detalles evaluados para la certificación.
- Module Type: Se indica si el módulo evaluado es un elemento físico (hardware) o si es una pieza de código (software). En este caso debemos tener en cuenta que se requieren hardware.
- Validation Date: Fechas en la que se emitió el certificado.
- Status: indica el estado del certificado.

Si un certificado de validación se marca como revocado, la validación del módulo ya no es válida y no se puede hacer referencia a ella para demostrar conformidad con FIPS 140-1 o FIPS 140-2. Por otro lado, si un certificado de validación se marca como histórico, la Universidad no debería tenerlos en cuenta para nuevas adquisiciones. Esto no significa que los certificados generales FIPS-140 para estos módulos hayan sido revocados, sino que indica que los certificados y la documentación publicada con ellos tienen más de 5 años de antigüedad y no han sido actualizados para reflejar las últimas guías y / o transiciones. De igual manera esto puede no reflejar con precisión cómo se puede usar el módulo en modo FIPS. Las agencias pueden determinar el riesgo de continuar utilizando los módulos en esta lista en función de su propia evaluación de dónde y cómo se usa el módulo (Validated Modules, 2016).

A continuación, se detallan los pasos para verificar si el producto eToken 5100 cumple con el estándar FIPS 140-2 Nivel 2 o superior Overall:

Paso 1:

Una forma de verificar el producto es utilizando el número de certificado del dispositivo indicado en el ítem 2 del apartado “5.1.3.3.2 Requisitos Previos”. Por otro lado, si no se cuenta con este número se deberá buscar el producto por su marca y modelo, como indica la figura 17.

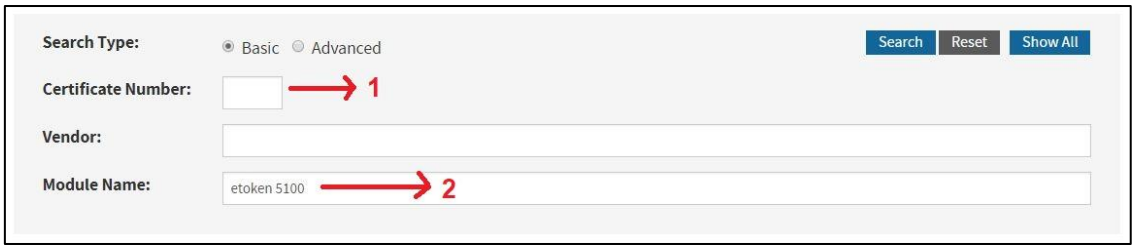


Figura 17: Buscador de NIST

Paso 2:

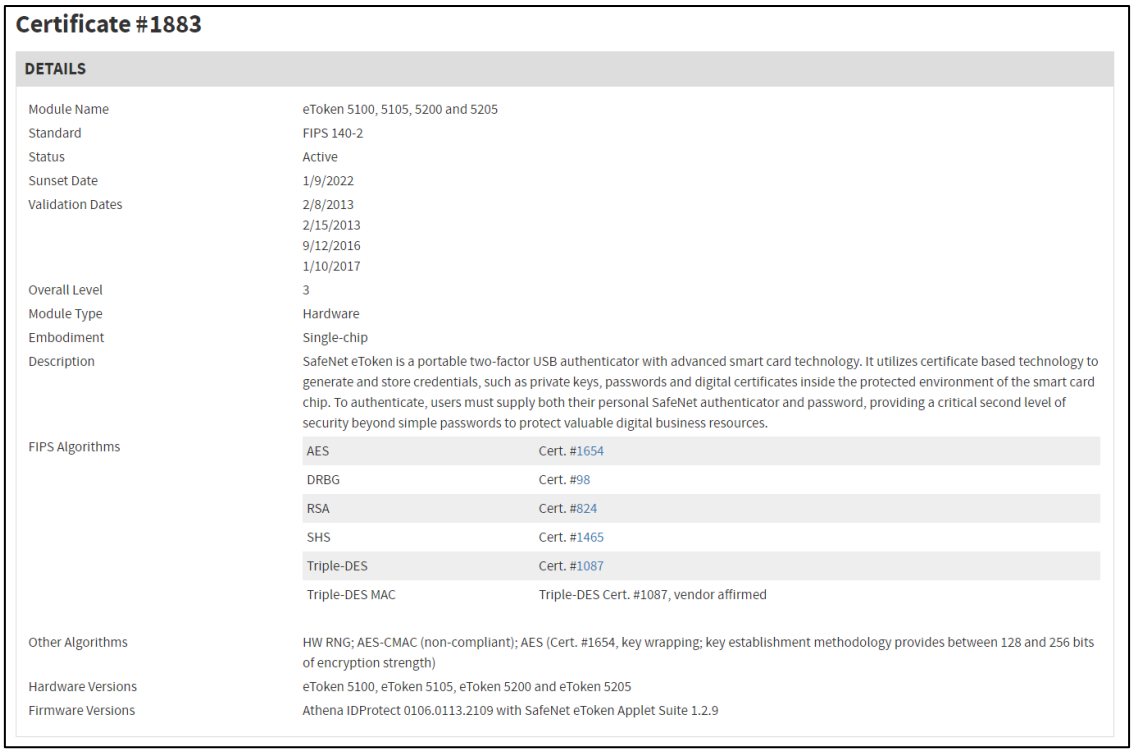
Según la figura 18, el dispositivo eToken 5100 cuenta el certificado nro. 1883. Además, se puede observar que tanto el nombre de la empresa (Vendor Name) y el producto (Module Name) son válidos, así como también el tipo del módulo (Module Type). A su vez, la fecha de última validación fue el 1 de octubre de 2017 y cuenta con un estado activo en su certificado de validación.

Certificate Number	Vendor Name	Module Name	Module Type	Validation Date	Status
1883	SafeNet, Inc.	eToken 5100, 5105, 5200 and 5205	Hardware	02/08/2013 02/15/2013 09/12/2016 01/10/2017	Active

Figura 18: Certificación del dispositivo eToken 5001

Paso 3:

Al hacer clic en el número de certificado de la imagen anterior, se puede observar con más detalles los lineamientos del producto, tal como muestra la figura 19.



Certificate #1883

DETAILS

Module Name	eToken 5100, 5105, 5200 and 5205
Standard	FIPS 140-2
Status	Active
Sunset Date	1/9/2022
Validation Dates	2/8/2013 2/15/2013 9/12/2016 1/10/2017
Overall Level	3
Module Type	Hardware
Embodiment	Single-chip
Description	SafeNet eToken is a portable two-factor USB authenticator with advanced smart card technology. It utilizes certificate based technology to generate and store credentials, such as private keys, passwords and digital certificates inside the protected environment of the smart card chip. To authenticate, users must supply both their personal SafeNet authenticator and password, providing a critical second level of security beyond simple passwords to protect valuable digital business resources.
FIPS Algorithms	AES — Cert. #1654 DRBG — Cert. #98 RSA — Cert. #824 SHS — Cert. #1465 Triple-DES — Cert. #1087 Triple-DES MAC — Triple-DES Cert. #1087, vendor affirmed
Other Algorithms	HW RNG; AES-CMAC (non-compliant); AES (Cert. #1654, key wrapping; key establishment methodology provides between 128 and 256 bits of encryption strength)
Hardware Versions	eToken 5100, eToken 5105, eToken 5200 and eToken 5205
Firmware Versions	Athena IDProtect 0106.0113.2109 with SafeNet eToken Applet Suite 1.2.9

Figura 19: Detalles del certificado de eToken 5100

Para finalizar con la verificación, se debe chequear si es estándar (Standard) utilizado es el FIPS 140-2 y si la descripción del campo Nivel General (Overall Level) es TRES (3).

De esta manera, se concluye que el dispositivo criptográfico eToken 5100 de la empresa SafeNet cumple con los requisitos de validación del estándar FIPS 140-2 hasta el 1 de septiembre de 2022.

5.1.4. Resumen del desarrollo del Plan en la UNRN

En resumen, la UNRN, en sus primeros pasos para convertirse en Autoridad de Registro perteneciente a la AC ONTI, deberá tener en cuenta:

5.1.4.1 Alcance

El plan contempla que tanto las autoridades de la UNRN como los cargos correspondientes a las Categoría I (uno), II (dos) y III (tres) del Escalafón No Docente, es decir que el Rector, Vicerrectores, Secretarios, Direcciones Generales, Direcciones y Jefaturas de Departamento, dispondrán de la Firma Digital cuyo certificado constará con un nivel de seguridad alto (ver Sección 3.3 “Verificación de Dispositivos Criptográficos (Token) bajo el estándar FIPS 140-2 Nivel 2 ó Superior.”)

5.1.4.2 Proyectos

A continuación, se detallan algunos de los proyectos que podrían contar con aplicaciones de Firma Digital en el ámbito de la UNRN. Si bien es una mera explicación, cada proyecto requerirá de un análisis detallado de los procesos que involucra, con el fin de adecuarlos y definir la correcta aplicación de la firma.

5.1.4.2.1 Recibo de sueldos digital

En la Universidad, se utiliza un sistema llamado Mapuche, promovido por el SIU (Sistema de Información Universitaria), para llevar a cabo la administración de la información del personal que trabaja en la misma. SIU-Mapuche (como se llamará de ahora en más) recoge toda la información de los recursos humanos de la institución en un Legajo Electrónico Único (sistema integrado), con el objetivo de brindar al operador todos los servicios necesarios para disminuir las posibilidades de error, facilitar el trabajo y evitar redundancias innecesarias, teniendo en cuenta los cambios en la legislación laboral vigente.

Mencionado lo anterior, la Universidad podría pretender confeccionar, firmar y distribuir los recibos de sueldo o haberes de forma digital mediante la plataforma SIU-Mapuche. La reducción de costo, la no utilización de papel y la baja demanda de tiempo que genera hacer lo anterior mencionado son los principales motivos para llevar a cabo este proyecto. Es decir que, este procedimiento, permitirá firmar digitalmente los recibos de sueldo de todos los docentes y nodocentes de la UNRN en cuestión de segundos. Así mismo, la Resolución 1455/11 del Ministerio de Trabajo de la República Argentina, habilita la posibilidad de la emisión de recibos de sueldo, a través de formas electrónicas o digitales, en reemplazo de soporte de papel, siguiendo los requisitos que la misma dispone. A fin de que un empleador pueda confeccionar los recibos de sueldo de esta forma, como primera medida la normativa establece que debe solicitarse por escrito ante la Secretaria de Trabajo autorización previa para la aplicación efectiva del nuevo formato, de acuerdo con los requisitos planteados en el art. 2° de dicha resolución (Bianchi, R. F., 2017).

5.1.4.2.2 Expediente electrónico

Se puede definir al expediente electrónico como un conjunto de documentos digitales correspondientes a un mismo proceso administrativo. Por otro lado, la gestión documental electrónica (de ahora en más GDE) consiste en la utilización de las tecnologías de la información y comunicación para facilitar el manejo, organización y preservación de la documentación digital producida y recibida por una organización.

Implementando un GDE, la Universidad podrá lograr una reducción en los tiempos de consulta y ejecución de las tareas que actualmente se realizan a partir de los archivos físicos. Además, se podrá mejorar la distribución de documentos entre los usuarios y las áreas centralizando la información,

garantizando el control y evitando la duplicidad. Un GDE ofrece estrategias, para asegurar los expedientes electrónicos, como la clasificación y parametrización de roles y permisos. Al desplazarse a un entorno digital y con la firma digital a la cabeza, la Universidad se convertirá en un modelo institucional de gestión documental y conciencia ambiental, reflejado en la creciente productividad.

Desde el punto de vista del proceso administrativo, un expediente generalmente se inicia en la Mesa de Entrada, se le coloca una carátula, un título y se le asigna un número. Este, denominado pedido de apertura, lo puede llevar a cabo un agente de la Universidad, ya sea un empleado o una autoridad, siempre y cuando se encuentre trabajando en planta. A medida que el trámite administrativo avanza, el expediente transita por distintas áreas y va ganando volumen a través de hojas de papel que son adosadas al final del mismo. Al superar las doscientas (200) hojas, se procede a la apertura de un segundo cuerpo del expediente.

Ese tránsito físico de oficina en oficina se irá reemplazando de a poco por un tránsito virtual. Cada área, departamento u oficina, en lugar de sumar una hoja, adjuntará un archivo digitalmente firmado. De esta manera, el sistema impuesto dejará constancia de la oficina por la que pasó el expediente, incluyendo la fecha y hora. La digitalización de los expedientes permitirá aumentar la eficiencia, ya que la remisión del mismo será de forma instantánea, sobre todo en una Universidad con sedes tan distantes. Además, el ahorro de tiempo en el circuito administrativo será considerable.

5.1.4.2.3 Digesto universitario

Digesto es término derivado del latín *digestum* que significa una compilación ordenada y codificada normas creadas por una institución. A su vez, un digesto permite acceder a todo lo actuado, sancionado y legislado en el tiempo constituyendo, así, el cuerpo de leyes o reglamentaciones por el cual se rige dicha institución.

Actualmente, el digesto de la UNRN se compone por: resoluciones rectorales, resoluciones de consejo, disposiciones de secretarías o secretarías de sede, entre otros documentos.

Con la implementación de la firma digital se espera formular un proceso gradual que adapte el actual digesto al mundo digital, con el objetivo de promover la integración de la información.

Con la creación del Repositorio Digital Institucional, ligado a la iniciativa de acceso abierto, la Universidad podrá resguardar el digesto producido y firmado digitalmente en un futuro. Si bien es un tema que se tratará más adelante en este capítulo, no estaba de más incluirlo.

5.1.4.2.4 Subir tesis de grado al Repositorio Institucional Digital

Para poder subir una tesis de grado al Repositorio Institucional Digital (RID), en primer lugar, el documento debe haber pasado por una instancia de evaluación por parte de la Universidad. En segundo lugar, el estudiante deberá acudir a las Ventanillas Permanentes (VP), es decir, a las oficinas de recepción de resultados de investigación, docencia y creación artística. Entre ellas se destacan: las bibliotecas de Sede, Secretarías de Investigación de Sede y el Departamento de Biblioteca, Repositorio y Contenidos Digitales (DBRyCD), que cumple con sus funciones en el edificio del Rectorado. Junto con el documento, en formato digital, el estudiante deberá presentar un formulario de cesión no exclusiva de derechos para depósito, bajo la licencia Creative Commons, y un formulario de registro de datos a modo de resumen del documento. Ambos formularios deben estar firmado por el remitente. Una vez realizado el trámite anterior, la VP hace entrega de un comprobante al estudiante con firma y sello de la Universidad, habiendo concluído éste con su papeleo.

Por otro lado, la VP remite los formularios DBRyCD y realiza la carga preliminar del documento digital. El DBRyCD cumplimenta la etapa de curaduría y realiza las devoluciones correspondientes en caso de ser necesario corregir y/o realizar modificaciones. Finalmente, el documento se sube al RID, se publica y se difunde (RID-UNRN, 2018).

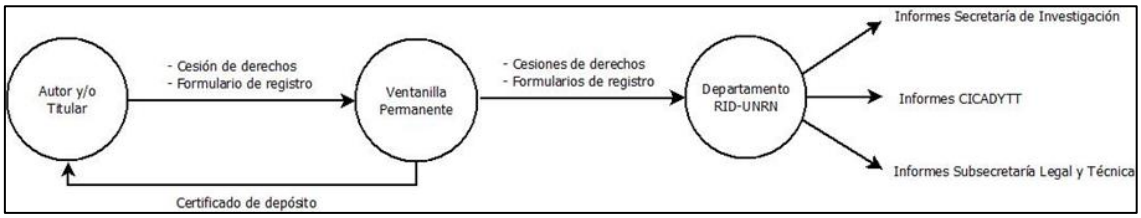


Figura 20: Proceso administrativo (RID-UNRN, 2018)

Actualmente, este proceso administrativo (ver Figura 20) demora entre 2 y 3 días en concretarse. Con la implementación de la firma digital, los estudiantes podrían emplear esta herramienta tanto para firmar su tesis como los formularios, y así enviarlos a través de correo electrónico a alguna de las VP disponibles, sin necesidad de estar físicamente en el lugar. A su vez, la VP podrá remitir el comprobante al alumno con su firma digital. De esta manera, no solo se reducirá el tiempo del trámite del estudiante en horas, sino que la tesis estará disponible en el RID con la firma digital del mismo.

5.1.4.2.5 Entrega de informes de proyectos de investigación

Los proyectos de investigación nacen de una convocatoria en la que cada director presenta su plan de proyecto detallando personal, herramientas y fondos económicos adecuados para llevarlo a cabo. Toda documentación del mismo

debe ser ingresada en el sistema SIGEVA de acuerdo a especificaciones fijadas por la SICADyTT, en un formato adecuado y con los formularios que contemplen su descripción técnica. Entonces, el proyecto es evaluado, por al menos cuatro investigadores calificados externos, y aprobado con dos o más votos positivos.

Aquellos proyectos aprobados deberán presentar anualmente un informe de avance (IA) o final (IF), dependiendo de su duración (anual, bienal o trienal), ante la Sede para su corrección y aprobación. Como se muestra en la Figura 21, actualmente, el proceso es el siguiente:

I. El director o codirector envía el IA o IF, en formato digital, a la Secretaría de Investigación de la Sede.

II. La Sede verifica el informe teniendo en cuenta: integrantes, fechas de baja o alta, disposiciones, formato del formulario, periodos de ejecución, etc., y comunica al investigador para su respectiva modificación.

III. El investigador realiza las correcciones al documento, y presenta una copia en digital y un original firmado a la Sede.

IV. El Secretario de Sede registra la entrada del documento y envía una copia escaneada a la SICADyTT (el informe en formato de papel solo se envía si el expediente asociado al proyecto se encuentra en el Rectorado).

V. Por su parte, la SICADyTT se encargada de recibir y verificar dichos documentos. El archivo digital se guarda en su correspondiente carpeta en la nube y el informe en papel en el expediente que corresponde.

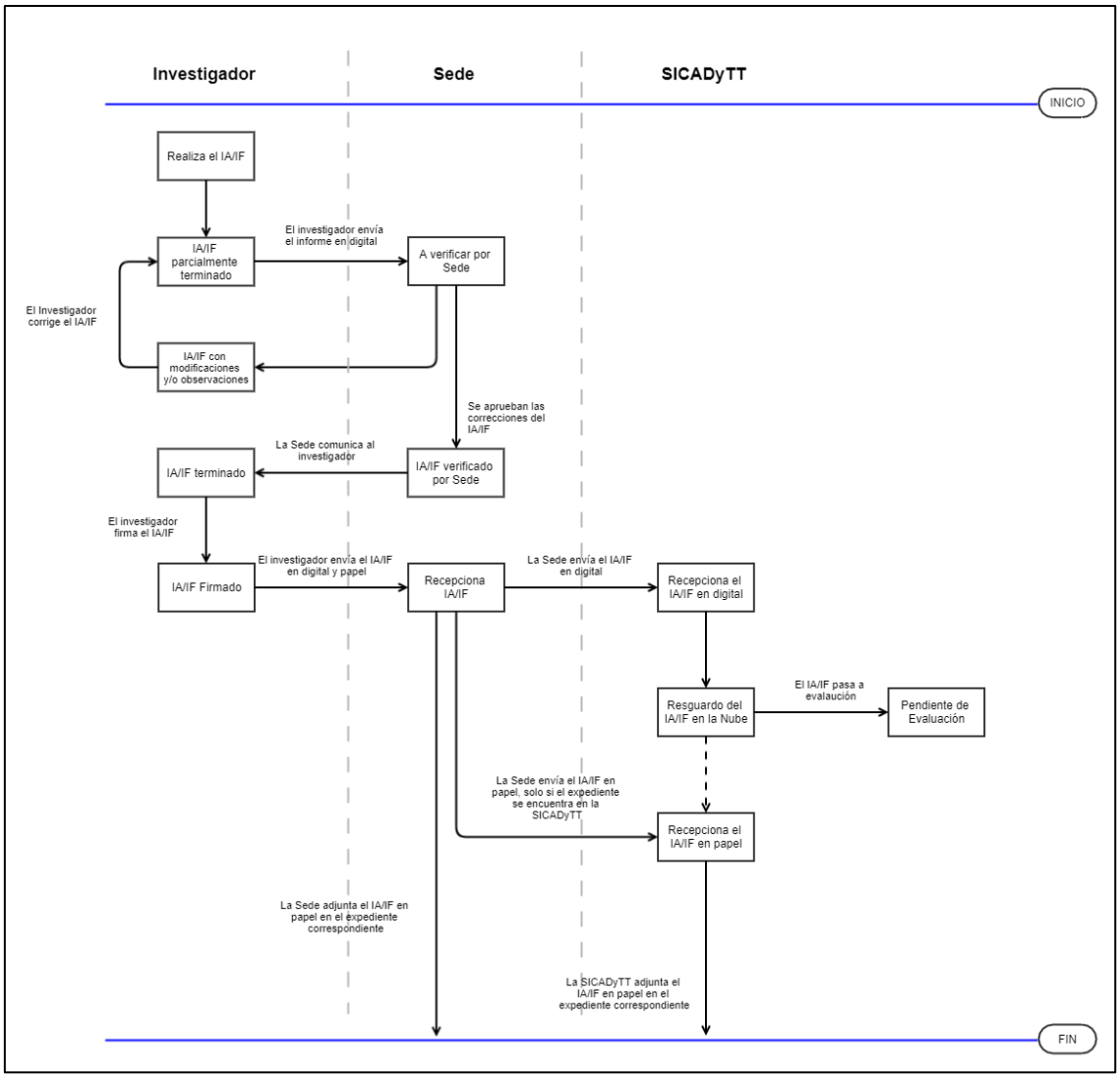


Figura 21: Proceso de recepción de IA y IF de los PI UNRN

Este proceso de entrega puede demorar días o meses, dependiendo de los investigadores y la Sede. Una vez que llegan a la SICADyTT, los informes pasan a la etapa de evaluación.

Con la implementación de la firma digital, tanto el director y/o codirector como el responsable de Sede podrían contar con un certificado digital que le permita firmar los informes. De esta manera, se reduciría el tiempo destinado a la transferencia de información. Por otra parte, la generación del expediente electrónico evitaría la presentación del informe en formato papel.

5.1.4.3 Actividades

5.1.4.3.1 Habilitar la modalidad móvil

A diferencia de la modalidad fija, la móvil permite al OR operar fuera del domicilio fijo declarado. Esto permitirá a la Universidad abarcar las Sedes sin la necesidad

de crear una Oficina de Registro en cada una. No solo será un cambio significativo en el presupuesto, sino que la documentación en papel generada estará centralizada.

5.1.4.3.2 Selección y capacitación de los Recursos Humanos

Los Responsables de la Autoridad de Registro deberán designar quien desempeñará los cargos de los Oficiales de Registro y del Soporte de Firma Digital, teniendo en cuenta la figura. Estos recursos humanos deberán ser previamente capacitados, con la obligación de aprobar el curso de capacitación detallado en el apartado 5.1.2.5 del presente.

5.1.4.3.3 Creación del expediente de firma digital

Por un lado, el art. 13° del Estatuto de la UNRN prevé la utilización de la Firma Digital en la administración con el objetivo de dotar de seguridad a las comunicaciones internas (UNRN, 2014, Art. 13°). Al ser este el único antecedente de la implementación de la firma digital en la Universidad, la misma deberá tomar medidas con respecto a la creación de un expediente como también en la redacción de información necesaria para reglamentar normas y reglas por las cuales se va a regir la institución. De este modo, se estudiarán los antecedentes y presentes de la Firma Digital con el objetivo de determinar qué normativa deberá ser incorporada y/o adaptada.

Con el objetivo de iniciar los trámites mencionados anteriormente en este apartado, se ideó un borrador de resolución de inicio de trámites de la Universidad contenido en el *Anexo A* de este documento.

5.1.4.3.4 Infraestructura de la Oficina de Registro

Si bien el “Manual de procedimientos” de la ONTI menciona requerimientos que debe cumplir la ubicación física de la Oficina de Registro de la Autoridad de Registro, el punto 5.1.2.7.2.1 del presente documento, define con mayor grado de detalle las características y materiales que debe tener dicha oficina. En caso de no optar por la modalidad de puesto móvil, cada sede de la Universidad deberá disponer de una oficina considerando dichas especificaciones. El correcto funcionamiento y acondicionamiento del Nivel 1 puede tardar aproximadamente dos semanas y corre por cuenta de la AR conformada. La AC ONTI se reserva el derecho de verificar dichas instalaciones en caso de considerarlo necesario.

5.1.4.4 Presupuesto a contemplar

Además de lo mencionado en el apartado *5.1.2.7.2.1 Requerimientos,* para acondicionar el Nivel 1, la Universidad deberá abastecerse de las siguientes utilidades:

- Un Armario Ignífugo.
- Una Computadora Personal con Windows 7 o superior original.
- Un Escritorio con uno o dos cajones.
- Dos sillas.
- Un aire acondicionado.
- Acceso con control biométrico.
- Una puerta blindada.
- Una UPS.
- Un Matafuegos de 5kg o 10kg.
- Una cámara IP
- Dispositivos criptográficos SafeNet eToken 5100 x20

Se debe tener en cuenta los gastos de instalación, cableado, materiales de obra para acondicionar la Oficina de Registro y viáticos para la capacitación del personal.

5.1.4.5 Tiempo estimado de conformación de la AR

Según la ONTI, el tiempo mínimo que tarda una institución o empresa en conformarse como AR es de dos meses.

1. Presentación de la documentación inicial, detallando Responsables de la AR, alcance de los proyectos que utilizarán firma digital y la designación de los Oficiales de Registro y Soporte de Firma Digital. Se estima una duración mínima de CATORCE (14) días abarcando la redacción de las notas, la creación de un expediente y la aprobación por parte del Rector
2. Capacitación de los Oficiales de Registro y Soportes Técnicos de Firma Digital: El curso se desarrolla en el Laboratorio de Firma Digital de la Ciudad Autónoma de Buenos Aires con duración de DOS (2) días consecutivos de DOCE (12) horas en total. A esto se le suma los días de traslado del personal de la Universidad quedando un total de CUATRO (4) días.
3. Exámenes: como se mencionó anteriormente, los exámenes son enviados por la AC-ONTI por correo electrónico. Los Oficiales de Registro

y Soportes Técnicos de Firma Digital tendrán hasta DIEZ (10) días para enviar las respuestas. Este plazo se puede prolongar en el caso de algún integrante no apruebe dicho examen.

4. Tramitación de los certificados: una vez aprobado los exámenes, los integrantes deberán concurrir a la AC-ONTI, con sede en Buenos Aires, para tramitar sus certificados digitales. Este proceso se podría demorar de UNA a DOS semanas, teniendo en cuenta la distancia, costos y disponibilidad de viaje.
5. Acondicionamiento del Nivel 1: como se especificó en el apartado *5.1.2.7.2 Operaciones de las Autoridades de Registro Fija,* la Oficina de Registro debe ser ambientada de una forma particular. Si bien es una actividad que puede llegar a tardar de DOS a TRES semanas, la Universidad deberá evaluar el espacio, el capital a invertir y su correcto acondicionamiento. La AC-ONTI se reservará el derecho de inspeccionar dichas instalaciones en caso de considerarlo necesario.
6. Habilitación de la AR: reunidas todas las consideraciones, la AC-ONTI procederá a habilitar a la Universidad como AR. Este trámite puede prolongarse hasta SIETE (7) días.

En resumen, el tiempo aproximado para conformar una AR es de dos meses como mínimo. Sin embargo, las estimaciones podrían variar de acuerdo con la gestión administrativa de cada entidad involucrada.

5.2 Herramientas de Firma Digital

La información teórica, tanto jurídica como técnica, se explicó en los anteriores capítulos de esta tesis, ahora corresponde incursionar en el terreno de lo práctico.

Por un lado, se llevará a cabo una introducción a las herramientas que emplean firma digital más utilizadas hoy en día, ya sean de uso libre o privativas, explicando cómo funcionan y cómo se diferencian a la hora de firmar documentos digitalmente. Por otro lado, se realizará una reseña de cómo almacenar dichos documentos teniendo en cuenta el grado de privacidad de cada uno.

5.2.1 Herramientas

Existen diversas herramientas para firmar digitalmente, sin embargo, en los siguientes párrafos se describen algunas que podrían resultar de interés para su utilización en el ámbito de la UNRN.

5.2.1.1 Thunderbird

Es un cliente de correo[15] de código abierto, multiplataforma, muy potente y fácil de usar, lanzado al mercado en el año 2004 por la Fundación Mozilla[16], una organización sin ánimo de lucro dedicada a la creación de software libre.

Entre las características de Thunderbird, se destacan:

- Gestiona múltiples cuentas POP, IMAP, SMTP, NNTP y canales web desde una sola interfaz, mejorada con las carpetas inteligentes y el uso de pestañas.
- Potentes filtros de detección de correo basura y correo fraudulento (phishing).
- Un sistema de búsquedas basado en base de datos que localiza en segundos todos los resultados relevantes entre decenas de miles de mensajes, con avanzadas herramientas de análisis.
- Filtros de mensajes para organizar tu correo fácilmente.
- Capacidad de redactar y visualizar mensajes HTML con el galardonado motor de representación Gecko[17].

[15] Un cliente de correo electrónico es un programa de ordenador usado para leer y enviar mensajes de correo electrónico.

[16] La Fundación también es el único accionista de Mozilla Corporation, el fabricante de Firefox y otras herramientas de código abierto. Mozilla Corporation funciona como una empresa social auto-sostenida: el dinero obtenido a través de sus productos se reinvierte en la organización. Para más información ver https://www.mozilla.org/en-US/foundation/

[17] Gecko es un motor de renderizado libre escrito en C++ y originalmente desarrollado por Netscape. Actualmente su desarrollo es gestionado por la Fundación Mozilla y la Corporación Mozilla.

- Libreta de direcciones con posibilidad de varias libretas separadas y conexión LDAP.
- Etiquetas y vistas de correo personalizables.
- Potente sistema de extensiones bajo el lema “donde Thunderbird no llegue, quizá lo haga una extensión” (Mozilla Corporation, 1998-2017).

Según Thunderbird, las "Firmas" son bloques de texto que se adjuntan automáticamente a cada mensaje que envíes (esto incluye tanto los nuevos mensajes como las respuestas a los mensajes entrantes) para proporcionar información de contacto adicional, términos legales o información repetitiva que sea necesaria en cada correo electrónico. Sin embargo, cuando se firma digitalmente un mensaje, se está introduciendo información en el mensaje que valida la identidad del emisor. Como se explicó en capítulos anteriores, cuando un mensaje es cifrado, este se muestra "mezclado e ilegible" y solo lo puede leer la persona que tiene la llave para descifrar dicho mensaje. La firma digital de un mensaje asegura que el mensaje salió desde el remitente esperado y el cifrado asegura que el mensaje no ha sido leído ni modificado durante su transmisión (Velo, A., 1998 - 2017).

A través del uso del protocolo Pretty Good Privacy (o PGP, basado en criptografía híbrida), Thunderbird emplea certificados digitales, los cuales equivalen a los documentos de identidad, para cifrar y descifrar la información transferida entre los sitios web. Así mismo, permite asociar cada cuenta de correo configurada con un certificado digital. También utiliza servidores de respuesta OCSP para confirmar el estado de los certificados actuales y así poder validarlos

5.2.1.2 Adobe Acrobat Reader DC

El software Adobe Acrobat Reader DC es el estándar gratuito de confianza para ver, imprimir, firmar y realizar anotaciones en archivos PDF. Es el único visor de PDF que permite abrir e interactuar con todos los tipos de contenido PDF, incluidos formularios y multimedia (Adobe Acrobat Reader DC, 2017).

Adobe permite el firmado de documentos electrónicos de tipo PDF de forma muy fácil integrando el estándar de Firma electrónica avanzada PDF (PAdES, por sus siglas en inglés). PAdES añade estampas de tiempo, cadenas de certificados y la información de revocación a los documentos firmados digitalmente, lo que permite verificar su validez en un futuro incluso si las fuentes originales (de consulta de certificados o de listas de revocación) no estuvieran disponibles, garantizando así la robustez tecnológica que brinda validez legal a la firma digital del documento electrónico en el tiempo (Álvarez C., M., 2015).

Con Adobe Reader se puede firmar digitalmente archivos PDF de forma gratuita no dependiente del sistema operativo. Sin embargo, es necesario instalar y configurar previamente los certificados digitales o jerarquía de certificación.

5.2.1.3 LibreOffice

LibreOffice es un Software Libre de ofimática[18] el cual incluye procesador de texto, planilla de cálculo y editor de presentaciones entre otras. LibreOffice nace como un desprendimiento de OpenOffice y, actualmente, es impulsado y desarrollado por su comunidad de software libre, bajo un proyecto de la organización sin fines de lucro, llamada The Document Foundation (LibreOffice, 2017).

LibreOffice permite firmar digitalmente documentos, lo que aporta seguridad al receptor de un documento de que ese documento no ha sido modificado y proviene del firmante del mismo. La firma digital corresponde a una firma normal, con las mismas consecuencias legales.

Al igual que Adobe Reader, LibreOffice necesita tener previamente el certificado configurado e instalado en la computadora. La gran diferencia con la aplicación de Adobe es que LibreOffice soporta firmas múltiples, es decir, varias personas pueden firmar digitalmente un mismo documento.

5.2.1.4 SIU-Toba: Firmador Digital

El Sistema de Información Universitaria o SIU es un consorcio, integrado por Universidades Nacionales Públicas, que desarrolla soluciones informáticas y brinda servicios para el Sistema Universitario Argentino. Así mismo, SIU-Toba es una herramienta de desarrollo que permite crear sistemas transaccionales en forma rápida, utilizando tecnología web open-source. El sistema apunta a agilizar el proceso de construcción y el mantenimiento de los mismos, a través de la reducción de tareas repetitivas, permitiendo al desarrollador enfocar su actividad en la lógica del dominio (SIU-Toba, 2015).

El firmador digital de SIU-Toba es un desarrollo basado en el firmador pdf de la ONTI (actualmente no se encuentra en internet) y utiliza tecnología de Applets de Java. Entre sus funcionalidades presenta:

- Funciona con un token-usb o keystore del navegador/SO.
- Permite firmar un único o múltiples documentos individuales.
- Valida la vigencia de certificados y OCSP (chequeo certificados revocados).
- Chequea la cadena de certificados (trusted-certificates).
- Visualización en línea del documento (si lo permite el navegador).

[18] Según la RAE, la palabra ofimática hace referencia a la automatización, mediante sistemas electrónicos, de las comunicaciones y procesos administrativos en las oficinas.

- Integración sencilla con aplicaciones (ejemplos con PHP standalone y SIU-Toba).

En la actualidad, los servicios de firma digital cuya tecnología se basa en Applets de Java son los más utilizados. La principal ventaja de esta tecnología es que pueden ejecutarse en un navegador web utilizando la Java Virtual Machine (JVM), o en el AppletViewer de Sun, es decir que cuando un navegador carga una página web que contiene un applet, este se descarga en el dicho navegador y comienza a ejecutarse. Si bien para su ejecución requiere un plugin de Java, navegadores como Chrome y Edge (sucesor de Internet Explorer) dejaron de dar soporte a los plugins basados en estándares (lo que excluyó la posibilidad de insertar Silverlight, Java, Flash y otras) y Firefox dejará de soportarlos próximamente. A causa de ello, Oracle, empresa que desarrolla el lenguaje de programación Java, anunció que abandonará el desarrollo del plugin de Java a partir de la salida de Java 9 (Bright, P., 2016).

El proyecto de firmador digital es de código abierto y se encuentra disponible en el repositorio Github: https://github.com/mecpy/firma-digital

Existen muchas herramientas hoy en día para firmar digitalmente, aunque en este apartado se mencionan las más importantes. Los firmadores, basados en la tecnología de Applets, todavía son los más utilizados y en su mayoría son de uso gratuito.

En resumen, Thunderbird sirve para firmar correos electrónicos, Adobe Reader para firma PDF, LibreOffice para firmar cualquier archivo de ofimática soportando multifirma, mientras que el Firmador de SIU-Toba firma cualquier tipo de archivo. Por lo tanto, quedará a disposición de la Universidad elegir la herramienta que más se adecúe a su funcionalidad.

5.2.2 Repositorio

Si bien la Universidad no almacenará los certificados digitales de sus agentes (sino la AC ONTI, como se mencionó anteriormente), necesita hacer uso de un repositorio para preservar el contenido firmado digitalmente que vaya generando.

5.2.2.1 Repositorio Digital

Los repositorios de contenidos digitales, también llamados bibliotecas digitales, son lugares donde se almacenan colecciones de recursos digitales de forma organizada con un sistema descriptivo a través de metadatos[19]. Estos repositorios almacenan los llamados objetos de información, que pueden ser

[19] Los metadatos son un conjunto de atributos que sirven para definir la información que se almacena dentro de un recurso de tal manera que se pueda catalogar y categorizar

textos, imágenes, videos, audio o cualquier archivo que pudiese contener información. Además, los repositorios digitales hacen uso de Internet para facilitar el acceso y la difusión de sus contenidos por parte de sus usuarios (Chazarra-Bernabé, Requena-López & Valverde-Jerónimo, 2010, p.10).

En base a lo anterior, la Universidad Nacional de Río Negro implementó un Repositorio Institucional Digital (RID), en el marco de la Ley Nacional 26899 de Repositorios Digitales con el propósito de maximizar la visibilidad, el uso y el impacto de la producción científica, académica y artística, apoyar el proceso de retroalimentación en el campo de la investigación, el arte y la cultura, así como facilitar el acceso a la información científica tecnológica. De esta manera el denominado RID-UNRN se adhiere a la iniciativa de Open Access (Acceso Abierto), que sustenta el principio de libre disposición de la información (Resolución CICADyTT N° 019, 2017).

Técnicamente hablando, el repositorio de la Universidad utiliza Dspace, un software destinado a organizaciones académicas, sin fines de lucro y comerciales que construyen repositorios digitales abiertos. DSpace es de código abierto, diseñado por el Massachusetts Institute of Technology (MIT) y los laboratorios de Hewlett Packard (HP), para gestionar repositorios de ficheros (textuales, audio, vídeo, etc.), facilitando su depósito, organización, asignación de metadatos y permitiendo también su difusión a recolectores o agregadores. Estas características han hecho que Dspace sea uno de los programas preferidos por las instituciones académicas para gestionar el repositorio donde los investigadores depositan sus publicaciones y materiales de búsqueda con objeto de darles una mayor visibilidad (Rodríguez-Gairín & Sulé-Duesa, 2008).

Sin embargo, para el proyecto mencionado en el apartado 5.1.4.3.1, RID-UNRN no cumple con las condiciones necesarias para albergar los recibos de sueldo, ya que al adherirse a la política de Open Access los recibos de sueldo tendrían que ser públicos. Por otra parte, el repositorio está en proceso de albergar el digesto de la Universidad, diferenciando entre resoluciones, disposiciones y normativas, entre otras, y así poder publicarlos, a futuro, con la firma digital de la o las autoridades correspondientes.

5.2.2.2 Gestor de contenidos

Para solventar el problema del archivado de recibos de sueldo se recomienda la utilización de gestores de contenidos y, de esta manera, brindar acceso fácil, rápido y seguro a los recibos de haberes para los agentes de la Universidad. En comparación, un repositorio es una herramienta para documentos digitales finales (llamados *records* en la jerga), mientras que un gestor de contenidos es un repositorio digital que gestiona la vida de un documento desde que nace hasta que se convierte en un *record*.

Por otra parte, los beneficios que presenta la utilización de firma digital integrada con un Sistema Software de Gestión Documental pueden ser:

1. Incrementar la productividad y eficiencia de los empleados.
2. Facilitar un entorno “sin papel” o “papel cero”.
3. Eliminar el riesgo de apropiación indebida de propiedad intelectual.
4. Alto retorno de la inversión, ahorro de costos significativo.
5. E-Archivado (Archivado Electrónico) de documentos legales.
6. Facilidad de acceso a la información.
7. Ahorro de impresión de miles de papeles al día (Meza, 2010).

5.2.2.2.1 Nuxeo

SIU-Mapuche, a partir de la versión 2.2.0 de enero de 2015, provee la utilización de firma digital para los archivos generados por el sistema que se encuentran almacenados en Nuxeo, gestor de contenidos recomendado por SIU. Fundada en el año 2000, la empresa Nuxeo se compone como una compañía global de software que ofrece una plataforma de gestión de contenidos para aplicaciones empresariales, denominado Nuxeo Platform.

Nuxeo Platform es un software modular de código abierto, desarrollado tanto por Nuxeo como por una comunidad de contribuidores, bajo LGPL (Lesser General Public License, o traducido como Licencia Pública General Menor), una licencia no recíproca de código abierto y libre aprobada como tal por la Free Software Foundation y la Open Source Initiative. Nuxeo Platform utiliza bibliotecas de terceros, principalmente de los proyectos Apache, JBoss y Eclipse, pero también del proyecto Java, ya que todas estas librerías usan licencias de código abierto que son compatibles con LGPL.

Si bien el software que provee Nuxeo es libre, su modelo de ingresos se basa en un programa de suscripción diseñado para ofrecer soporte, mantenimiento y servicios al cliente y a la comunidad de socios, comúnmente denominado SaaS (Software as a Service, Software como Servicio). De este modo, Nuxeo, presenta dos opciones para llevar a cabo la utilización de su sistema, ya sea pagando el servicio que ofrece su empresa o no. En caso de que se eligiera lo segundo, la configuración, instalación y mantenimiento del software correrá por cuenta de la Universidad.

5.2.2.2.2 Alfresco

Al igual que Nuxeo, Alfresco es un software para la Gestión de Contenido Empresarial (o, en inglés, Enterprise Content Management) de código abierto con licencia LGPL, modular y escalable basado en estándares abiertos como Java, Apache, JBoss, Lucene, OpenShare, entre otros. Cuenta con dos versiones disponibles: Alfresco Community Edition y Alfresco Content Service (que es la versión SaaS).

En la versión Community, el software de código abierto de Alfresco ha sido ampliamente adoptado para el desarrollo gracias a las contribuciones de la comunidad, así como para la investigación de nuevas características. Si bien la asistencia corre por cuenta de la Universidad, provee un control de calidad limitado de Alfresco, también de código abierto distribuido con licencia LGPL, con corrección de errores únicamente para la versión actual.

A diferencia de Nuxeo, el software Alfresco ya fue utilizado anteriormente por la Universidad y se conoce tanto su funcionamiento como sus requerimientos y configuración a la hora de la instalación. Por otra parte, la ventaja de Nuxeo es el apoyo que tiene por parte del SIU al considerarlo para la herramienta Mapuche, brindando soporte y asistencia a través de su foro. En resumen, queda a disposición de la Universidad elegir cuál de los ECM se adapta mejor a su arquitectura y funcionalidad.

5.2.2.3 OwnCloud: almacenamiento en la nube

Los gestores de contenidos pueden resultar complejos por la diversidad de funciones que presentan a la hora de cargar, modificar o versionar un archivo. Como alternativa de manejo simple para los usuarios finales se plantea una solución de almacenamiento en la nube. La nube o computación en la nube es el término dado a los servidores de internet que se encargan de almacenar y procesar datos, el cual proviene de su expresión en inglés Cloud Computing.

OwnCloud es una aplicación de software libre de almacenamiento privado con acceso restringido, desde cualquier dispositivo, a los archivos que se encuentran disponibles a través de internet. El proyecto fue lanzado en enero del 2010 por Frank Karlitschek con el objetivo de brindar una alternativa económica, escalable, flexible y segura. OwnCloud provee una interfaz de usuario donde podrá subir, compartir, buscar y etiquetar archivos, entre otras funciones.

Al ser de código abierto, la Universidad podrá configurar OwnCloud dentro de sus instalaciones brindando un servicio de almacenamiento de archivos para sus agentes. De esta manera, podrá modificar características como el diseño, o limitar funciones de la forma que se considere correspondiente.

5.2.3 Guías de uso de la Firma Digital en la Universidad

Partiendo de que la firma digital es un procedimiento poco conocido en la Universidad, los futuros usuarios podrían sentirse desorientados y con falta de información para utilizarla. De esta manera, cuando se constituya la AR, la Universidad deberá tener en cuenta el desarrollo de los siguientes manuales de usuario:

- Instalación del certificado en la computadora: este abarca todos los procedimientos a seguir desde que se solicita una firma digital en la AR-

UNRN, hasta la instalación del certificado digital en la computadora o token.

- Firmar un archivo: se llevarán a cabo los pasos para firmar de forma digital un archivo utilizando alguna de las herramientas mencionadas en el apartado 5.2.1
- Firmar un correo electrónico: el cual explicará cómo firmar digitalmente un correo electrónico mediante la utilización de un cliente de correo.
- Verificar una firma digital: ya sea en un mensaje de correo electrónico como en un archivo de ofimática.

Es importante mencionar que en el primer manual se describe tanto el proceso específico de la solicitud de una firma digital como la instalación de los certificados de la AC ONTI y de la RAÍZ. Es necesario que los datos personales que se proporcionen para la emisión del certificado sean totalmente verídicos, para que no sea negada la solicitud por parte de la AC ONTI. Como la firma digital se basa en la confianza de esta entidad prestadora de servicios de certificación, algunos programas pueden mostrar algún tipo de alerta de seguridad, por no tener a la autoridad certificadora dentro la lista de AC confiables; por ello, es importante agregar el certificado tanto de la AC ONTI como el de la AC RAÍZ para que el programa no muestre falsas alertas.

Sin más, la Universidad deberá crear los manuales que le sean suficientes para que el personal puede entender, diferenciar y emplear la firma digital dentro de la institución, siguiendo los lineamientos de esta tesis de grado.

Capítulo 6: Conclusiones y recomendaciones futuras

Para finalizar este trabajo de tesis sólo resta expresar las conclusiones obtenidas de los temas abordados. De igual forma se describen algunas líneas futuras de investigación, que no alcanzaron a ser desarrolladas en el presente trabajo.

6.1 Conclusiones

Hoy en día, no puede negarse el constante avance de la tecnología que ocasiona que distintas empresas y/o organismos trasladen sus procesos al mundo digital. De la misma manera, la Universidad no debe quedarse atrás. No estamos frente al reto de proteger un gran sistema central de información administrado. Tampoco se trata de manejar grupos reducidos y estáticos de personas, ni de controlar una simple carpeta compartida. Por el contrario, en el entorno actual de la Universidad se encuentran una gran cantidad de usuarios, geográficamente separados, que desean acceder a un número creciente de recursos administrados en papel.

La gran cantidad de documentos que se gestiona en la actualidad causa retrasos y, a veces, pérdidas de estos, que pueden ser solventados con la utilización de documentos digitales. Los beneficios que acarrean estos últimos parten desde el costo, distribución, almacenamiento hasta su generación. Sin embargo, sus peligros también están relacionados con la autentificación, integridad y el no repudio de éstos.

Hay que tener en cuenta que la Firma Digital no busca reemplazar a la firma hológrafa, pero proporciona al documento digital las garantías jurídicas y legales que hasta ahora gozaban los documentos firmados en papel. Al igual que la firma hológrafa, la firma digital no puede asegurar la confidencialidad de un documento, pero puede brindar la integridad de este.

De esta forma, la implementación de la firma digital agilizará los procesos de firma de documentos, logrando una gestión más eficiente al reducir los tiempos sin la necesidad de la presencia física de las partes. Un agente de la Universidad, desde cualquier lugar, podrá tener acceso a la infraestructura necesaria, hacer uso de la Firma Digital y permitir que la documentación siga su rumbo, con el objetivo de poder lograr los resultados que la misma se propone.

Debido a la importancia de todo lo que se pone en juego con un proyecto de tal magnitud, la decisión más correcta, es la de implementar la firma digital a través

de la constitución de una Autoridad de Registro. Se tiene conciencia de la gran inversión que esto requiere: en capital, tiempo, tecnología y personal calificado, pero es imprescindible, para poder ofrecer todas las garantías necesarias. Luego de la inversión inicial requerida, la digitalización de la documentación que se utiliza y/o utilizará en los distintos procesos, genera la reducción de costos en lo referido a captura, administración, mantenimiento y archivo de la información, pero, sobre todo, en el tiempo destinado para hacerlo (Pérez, 2009).

La digitalización de la información brinda ventajas en materia de acceso a los datos, por lo que es importante desarrollar una cultura de compartir la información entre los distintos departamentos de la Universidad. Hoy existe aún mucha desconfianza y dudas respecto a la seguridad que los medios digitales poseen y que, fundamentalmente, se deben a falta de información clara y precisa. No se confía en lo que no se conoce. Para reducir esta brecha de la incertidumbre, hay que ser capaz de integrar los conceptos de la firma digital y poder transmitirlos. Un fuerte plan comunicacional y de docencia para que ésta propuesta de innovación sea conocida y adoptada naturalmente por los empleados de la Universidad, ligada a la formulación de manuales de usuario y el desarrollo de cursos, son herramientas útiles y necesarias para lograrlo.

La Firma Digital constituye una transformación progresiva e integral en el modo de trabajo que las personas desarrollan dentro de la Universidad. Es decir, implica repensar el modo en el que se desarrollan las tareas, enfocándose hacia procedimientos mucho más dinámicos y eficientes.

Todas las herramientas tecnológicas incluida la Firma Digital no son nada por sí mismas, sino que van acompañadas por un cambio de paradigmas en cuanto al desarrollo de procesos y procedimientos. (Pérez, 2009).

Por otro lado, existen una variedad de herramientas pagas y gratuitas en el mercado que permiten firmar digitalmente. La Universidad tendrá el desafío de optar por alguna de ellas o desarrollar una propia, teniendo en cuenta la futura desaparición de los applets de Java.

La obligatoriedad de utilizar un procedimiento digital puede ser una alternativa para dar los primeros pasos, pero no debe ser la regla. Existen sobrados ejemplos en el mundo donde se ha buscado imponer el uso de herramientas digitales y se ha fracasado, derrochando enormes cantidades de dinero invertidas en su desarrollo e implementación (Dergarabedian, 2018). Si bien Argentina fue pionera, en América Latina, en la formulación de leyes de Firma Digital, tardó demasiado en implementarla, dado que la adopción de las tecnologías informáticas requiere un proceso de adecuación de los distintos recursos, tanto humanos como materiales. Sin embargo, la Universidad no tiene

que seguir el mismo camino. En la actualidad, cuenta con equipamiento y recursos necesarios para llevar a cabo el proyecto de implementar la firma digital correctamente.

6.2 Avances

En el transcurso de esta tesis, la Secretaría de Programación y Gestión Estratégica de la UNRN realizó los trámites iniciales para llevar a cabo la conformación de la Autoridad de Registro, que dependerá directamente de la ONTI. Las actividades realizadas fueron:

- Se estableció contacto con la ONTI por medio del correo electrónico consultapki@modernizacion.gob.ar, con el fin de solicitar los modelos de notas detallados en el apartado *5.1.2.5 Procedimiento de conformación de la Autoridad de Registro*.
- Con los modelos en mano, se formularon las notas correspondientes a la designación de los Responsables de la Autoridad de Registro, los Oficiales de Registro y habilitación de la modalidad móvil. En las mismas se especifica al recibo de haberes, el expediente electrónico y el digesto universitario son los proyectos que inicialmente implementarán firma digital. Una vez firmadas por el Rector, máxima autoridad de la Universidad, las notas se enviarán a la ONTI y así continuar con los pasos detallados en esta tesis.
- Se asignó la apertura del expediente 1499/2017 denominado “Proyecto Firma Digital UNRN” incluyendo la normativa vigente de Firma Digital de Argentina al 13 de diciembre de 2017.
- En el mes de abril de 2018, algunos Oficiales de Registro se capacitaron y tramitaron sus certificados digitales.

Capítulo 7: Referencias bibliográficas

Álvarez C., M. (2015, 14 de mayo). Guía de Firma Digital para Adobe Reader DC. Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT). Costa Rica. Recuperado el 23 de octubre de 2017, de: http://www.bccr.fi.cr/firma_digital/guiaAdobe.pdf

Amieva, E. (2015, 13 diciembre). Criptografía: simétrica, asimétrica e híbrida. Recuperado el 7 de septiembre de 2017 de: https://enekoamieva.com/wp-content/uploads/2015/12/cifrado-simetrico.png.

Bates, B. N. (2014, 13 de noviembre). Why an E-signature is Actually More Secure than a Physical Signature. eSignLive. Recuperado el 13 de febrero de 2018, de: https://www.esignlive.com/blog/e-signature-actually-secure-physical-signature

Bianchi, R. F. (2017, 10 de marzo). Qué deben saber los empleadores para emitir recibos de sueldos de manera digital. iProfesional. Recuperado el 23 de octubre de 2017, de: http://www.iprofesional.com/notas/246792-Que-deben-saber-los-empleadores-para-emitir-recibos-de-sueldos-de-manera-digital.

Bienvenidos a Firma Digital San Juan (s.f). Autoridad de Registro de Firma Digital del Gobiern de la Provincia de San Juan. Recuperado el 11 de marzo de 2018, de: http://www.dgrhyo.sanjuan.gov.ar/fd_firma_digital.php

Blanco, E. (2011, 11 de abril). Avanza el proyecto Mercosur Digital. Portinos. Recuperado el 28 de septiembre de 2017 de: https://portinos.com/tecnologia/avanza-el-proyecto-mercosur-digital.

Bright, P. (2016, 27 de enero). Oracle deprecates the Java browser plugin, prepares for its demise. Ars Technica. Recuperado el 23 de octubre de 2017, de: https://arstechnica.com/information-technology/2016/01/oracle-deprecates-the-java-browser-plugin-prepares-for-its-demise/

Carbone, F. (2016, 06 de junio). La firma digital avanza y gana terreno en la Argentina. La Nación. Recuperado el 28 de septiembre de 2017 de: http://www.lanacion.com.ar/1905686-la-firma-digital-avanza-y-gana-terreno-en-la-argentina.

Chazarra-Bernabé, J., Requena-López, V. M. & Valverde-Jerónimo, S. (2010). Desarrollo de un repositorio de objetos de aprendizaje usando DSpace. Universidad Complutense de Madrid. Recuperado el 23 de octubre de 2017, de: http://eprints.ucm.es/11078/1/MemoriaSI.pdf

RID-UNRN (2018). ¿Cómo subir un documento al RID-UNRN? Repositorio Institucional Digital de la Universidad Nacional de Río Negro. Recuperado el 24 de marzo de 2018, de: http://rid.unrn.edu.ar/jspui/como%20subir.jsp

Resolución CICADyTT N° 019/2017 (2017, 27 de junio). Concejo de Investigación, Creación Artística y Transferencia de Tecnología. Universidad Nacional de Río Negro, San Carlos de Bariloche.

Decreto N° 2628/2002. (2002, 19 de diciembre). "Reglamentación de la Ley N° 25.506 (...)". Administración Pública Nacional. Argentina. Recuperado el 28 de septiembre de 2017 de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/80000-84999/80733/norma.htm.

Decreto N° 427/1998. (1998, 16 de abril). "Régimen al que se ajustará el empleo de la firma digital (…)". Administración Pública Nacional. Argentina. Recuperado el 27 de septiembre de 2017 de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/50000-54999/50410/norma.htm.

Dergarabedian, C. (2018, 1 de marzo). Firma digital: "No se confía en lo que no se conoce". iProfesional. Recuperado el 24 de marzo de 2018, de: http://www.iprofesional.com/notas/264168-software-celular-pc-tableta-hardware-firma-digital-modernizacion-firma-digital-remota-gestion-documental-electronica-Firma-digital-No-se-confia-en-lo-que-no-se-conoce?page_y=0

De León, M. & Timón, A. (2014, 30 de junio). Números primos: los guardianes de Internet. Ciencia para llevar: El blog del CSIC. Recuperado el 13 de marzo de 2018 de: https://blogs.20minutos.es/ciencia-para-llevar-csic/2014/06/30/numeros-primos-los-guardianes-de-internet/

De Luca, J. C (2015). La implementación de la firma digital en el sector público: mejoras en la gestión y en los procesos para lograr óptimos resultados. Facultad de Ciencias Económicas, Universidad de Buenos Aires.

Diffie, W. & Hellman, M. E. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory, IT-22(6):644-654.

Electronic Frontier Foundation (1998, 8 de julio). Cracking DES: secrets of encryption research, wiretap politics & chip design. CA: O'Reilly, Sebastopol.

Ente Licenciante - Argentina. (s.f). Gobierno de la República Argentina. Recuperado el 26 de septiembre de 2017, de: https://www.argentina.gob.ar/firmadigital/entelicenciante

FIPS 140-2. (s.f.). En Wikipedia. Recuperado el 02 de octubre de 2017 de: https://es.wikipedia.org/wiki/FIPS_140-2.

González, J. L. (2007, 5 de julio). Qué diferencia a la firma digital de la electrónica. iProfesional. Recuperado el 23 de octubre de 2017, de: http://www.iprofesional.com/notas/49143-Que-diferencia-a-la-firma-digital-de-la-electronica

Hauria, M. (2014, 17 de noviembre). Ventajas del creciente uso de la firma digital en la sociedad digital de Argentina. CanalAR. Recuperado el 28 de septiembre de 2017 de: http://www.canal-ar.com.ar/eresnoticia.asp?Id=5595.

Agencia de Noticias de San Luis (2017, 31 de agosto). Importante empresa privada comenzó a usar la firma digital. Recuperado el 29 de septiembre de 2017, de: http://agenciasanluis.com/notas/2017/08/31/importante-empresa-privada-comenzo-a-usar-la-firma-digital/

Ley 25506. (2001, 11 de diciembre). Ley de Firma Digital. República Argentina

Litwak, N. D. & Escalante, J. E. (2004). Seguridad informática y criptografía. Univ. Nacional del Nordeste. Corrientes, Argentina. Recuperado el 8 de

septiembre de 2017, de: http://exa.unne.edu.ar/informatica/SO/Criptografia04.pdf.

Lucena López, M. J. (2010). Criptografía y Seguridad en Computadoras. Versión 4-0.8.1. Univ de Jaén, España.

Luna, M. (2012, 6 de octubre). Criptografía y los Diferentes Tipos de Cifrado [Web log post]. Recuperado el 13 de septiembre de 2017, de http://manuelluna08.blogspot.com.ar/2012/10/criptografia-y-los-diferentes-tipos-de_6.html.

Mercosur Digital crea nuevo escenario de comercio electrónico en Paraguay (2013, 1 de noviembre). La Nación, Paraguay. Recuperado el 26 de septiembre de 2017 de: https://politicacomunicada.com/mercosur-digital-crea-nuevo-escenario-de-comercio-electronico-en-paraguay.

Mesa Sánchez, A. (2015). Sistema de Firma Digital para el Ministerio de Obras Públicas, Servicios y Vivienda (Tesis de grado). Universidad Mayor de San Andrés. La Paz, Bolivia.

Meza, V. (2010, 24 de junio). Firma Digital. Blog de Captura y Gestión Documental Inteligente. Athento. Recuperado el 23 de octubre de 2017, de: http://blog.athento.com/2010/06/firma-digital.html

Molina, H. G. (2006). Avances en Informática y Sistema Computacionales Tomo I (CONAIS 2006). Univ. J. Autónoma de Tabasco. México. Recuperado el 30 de agosto de 2017, de: https://books.google.es/books?isbn=9685748985.

Mozilla Corporation (1998 - 2017). Características de Thunderbird. Mozilla.org. Recuperado el 23 de octubre de 2017, de: https://www.mozilla.org/es-ES/thunderbird/features.

Nishikawa, T. & Matsuoka, S. (2008). Time-Stamping Authority Grid. IEEE, vol. 7, p. 98 - 105.

Oficina Nacional de Tecnologías de Información (2015 A). Requerimientos para la conformación de las autoridades de registro de la AC ONTI. Versión 3.0. Jefatura de Gabinete de Ministros.

Oficina Nacional de Tecnologías de Información (2015 B). Manual de Procedimientos. Versión 2.0. Jefatura de Gabinete de Ministros. Recuperado el 02 de octubre de 2017, de: http://pki.jgm.gov.ar/docs/Manual_de_Procedimientos_ACONTIv2.0.pdf.

Pérez Jurado, G. (2009, 1 de mayo). Firma digital y sus implicancias en la despapelización del sector público. V Congreso Argentino de Administración Pública. Recuperado el 10 de noviembre de 2017, de: http://www.asociacionag.org.ar/pdfcap/5/

Adobe Acrobat Reader DC. ¿Qué es Adobe Acrobat Reader DC? (s.f.). Preguntas más frecuentes sobre Adobe Acrobat Reader DC. Recuperado de 23 de octubre de 2017, de: https://helpx.adobe.com/es/reader/faq.html

LibreOffice (2017). ¿Qué es LibreOffice?. LibreOffice: The Document Foundation. Recuperado el 23 de octubre de 2017, de: https://es.libreoffice.org/descubre/libreoffice/

Resolución GMC N° 37/06 (2006, Julio 18). Reconocimiento de la eficacia jurídica del documento electrónico, la firma electrónica y la firma electrónica avanzada en el ámbito del Mercosur. Grupo del Mercado Común (GMC). Mercosur. Recuperado el 25 de septiembre de 2017 de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/120000-124999/120555/norma.htm.

Resolución MM 399-E/2016 (2016, 5 de octubre). Firma Digital: Requisitos para el licenciamiento de certificadores y otros. Ministerio de Modernización, Argentina. Recuperado el 29 de septiembre de 2017, de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/266312/norma.htm.

Reverte, O. C (2002). Propuesta de una infraestructura de clave pública y su extensión mediante un sistema de gestión distribuida de credenciales basado en delegación y roles (Tesis Doctoral). Facultad de Informática, Univ. de Murcia, España.

Rivolta,M. & Bugoni, M. (2007). “e-Autenticación: firma digital y firma electrónica. Panorama en la República Argentina”. Observatorio de Políticas Públicas.

Rodríguez-Gairín, J. M. & Sulé-Duesa, A. (2008). "DSpace: un manual específico para gestores de la información y la documentación". BiD: textos universitarios de biblioteconomía y documentación, núm. 20 (junio). Recuperado el 24 de octubre de 2017, de: http://bid.ub.edu/20rodri2.htm

Salinas Hinojosa, K. D. (2013). Tokens de seguridad. Revista de Información, Tecnología y Sociedad (RITS) [online]. n.8, pp. 59-61. ISSN 1997-4044. Recuperado el 02 de octubre de 2017, de: http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442013000100025&script=sci_arttext.

Seagate (s.f). Tecnología estándar FIPS 140-2 y unidad de cifrado automático: preguntas frecuentes. Recuperado el 23 de abril de 2018, de: https://www.seagate.com/la/es/tech-insights/fips-140-2-standard-and-self-encrypting-drive-technology-master-ti/.

Sitio oficial Firma Digital de San Luis 3.0 (s.f.). Instituto Firma Digital de San Luis. San Luis, Argentina. Recuperado de: http://www.pki.sanluis.gov.ar/lafirma.html

Sitio web institucional Mercosur - En pocas palabras (s.f.). Mercosur - ¿Qué es el Mercosur?. Montevideo, Uruguay. Recuperado el 29 de septiembre de 2017, de: http://www.mercosur.int/innovaportal/v/3862/2/innova.front/en-pocas-palabras

SIU-Toba. (2015). Ambiente de Desarrollo Web. Sistema Universitario Nacional. Recuperado el 23 de octubre de 2017, de: https://www.siu.edu.ar/siu-toba/

TICPymes (2015, 9 octubre). Ventajas de implementar la firma digital. TICPymes. Recuperado el 9 de noviembre de 2017, de: http://www.ticpymes.es/tecnologia/noticias/1084464049504/ventajas-implementar-firma-digital.1.html

Universidad Nacional de Río Negro (2014, diciembre). Estatuto. Recuperado el 26 de octubre de 2017, de: https://www.unrn.edu.ar/images/Estatuto_UNRN_-_Vigente_diciembre_2014.pdf.

Urrego, E., Vargas Aguirre, M. & Echavarría, V. C. (2011). Propuesta de implementación de la firma digital para la Cooperativa Coopserp. Universidad de Medellín, Colombia.

Validated Modules (2016, 11 de octubre). Cryptographic Module Validation Program. NIST. Recuperado el 28 de octubre de 2017, de: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules.

Vallejos Arcos, C. A. (2003). Diseño de una PKI para el desarrollo de aplicaciones bancarias seguras sobre internet mediante firma digital (Tesis de grado). Universidad Austral de Chile. Valdivia, Chile.

Varela Velasco, R. D. (2006). Criptografía: una necesidad moderna. Revista digital universitaria, UNAM. Recuperado el 6 de septiembre de 2017, de: http://www.revista.unam.mx/vol.7/num7/art56/jul_art56.pdf.

Velo, A. (1998 - 2017). Firma digital y cifrado de mensajes. Foundation Mozilla. Recuperado el 23 de octubre de 2017, de: http://mzl.la/1BsOGiZ

Wang, X. & Yu, H. (2005). How to Break MD5 and Other Hash Functions. In: Cramer R. (eds) Advances in Cryptology – EUROCRYPT 2005. EUROCRYPT 2005. Lecture Notes in Computer Science, vol 3494. Springer, Berlin, Heidelberg

Anexo A: Notas y Resolución

El objetivo del anexo es mostrar los modelos de notas provistas por el Ministerio de Modernización y la propuesta de Resolución que podría presentar la Universidad, para iniciar los trámites de firma digital. Todas las notas deberán incluir el membrete de la Universidad.

A.1 Notas provistas por el MM

A.1.1 Conformación Autoridad de Registro 2017 (Firmada por Máxima Autoridad)

……., ….. de …….. de ……

REF: CONFORMACIÓN AUTORIDAD DE REGISTRO DE LA AC ONTI.

AL RESPONSABLE DE LA AUTORIDAD CERTIFICANTE DE LA

OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN

S / D

Me dirijo a Ud. a fin de solicitarle autorización y asistencia para la conformación de una Autoridad de Registro de la Autoridad Certificante ONTI a su cargo en ……..……, con el fin de implementar el uso de la firma digital en esta jurisdicción.

En tal sentido, asumimos el compromiso de cumplir con lo dispuesto en la Ley Nº 25.506, el Decreto N° 2628/2002 y sus modificatorios, la Resolución 399e/2016 del MINISTERIO DE MODERNIZACIÓN y 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.

Se informa que se implementará el uso de la firma digital en los siguientes proyectos:

……
..……
……..……..……
……

De mediar una respuesta favorable, y a fin de iniciar el procedimiento de conformación, informo a Ud. la designación de los siguientes funcionarios en su calidad de Responsables de la Autoridad de Registro:

- **RESPONSABLES DE LA AUTORIDAD DE REGISTRO**:

  - **Nombre y APELLIDO**, tipo y número de documento de identidad, CUIL/CUIT, cuenta de correo institucional, teléfono laboral de contacto.
  - **Nombre y APELLIDO**, tipo y número de documento de identidad, CUIL/CUIT, cuenta de correo institucional, teléfono laboral de contacto.
  - **Nombre y APELLIDO**, tipo y número de documento de identidad, CUIL/CUIT, cuenta de correo institucional, teléfono laboral de contacto.

Sin otro particular, saludo a usted atentamente.

.....

Firma, Aclaración y DNI

(Autoridad Máxima del Organismo Solicitante)

A.1.2 Designación de Roles AR 2017 (Firmada por Responsable AR)

……., ….. de …….. de ……

REF: DESIGNACIÓN DE ROLES, DOMINIO/S Y DOMICILIO/S - AUTORIDAD DE REGISTRO DE LA AC ONTI.

AL RESPONSABLE DE LA AUTORIDAD CERTIFICANTE DE LA OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN

S / D

El que suscribe, ……..., en mi carácter de Responsable de Autoridad de Registro de la Autoridad Certificante ONTI en el Organismo ……., tiene el agrado de dirigirse a Ud. a los fines de hacerle saber que se han designado a los siguientes funcionarios en los roles que a continuación se indican:

- **OFICIALES DE REGISTRO**:
  - **Nombre y APELLIDO**, tipo y número de documento de identidad, CUIL/CUIT, cuenta de correo institucional, teléfono laboral de contacto y número de serie del certificado digital …… (en caso de corresponder).
  - **Nombre y APELLIDO**, tipo y número de documento de identidad, CUIL/CUIT, cuenta de correo institucional, teléfono laboral de contacto y número de serie del certificado digital …… (en caso de corresponder).
  - **Nombre y APELLIDO**, tipo y número de documento de identidad, CUIL/CUIT, cuenta de correo institucional, teléfono laboral de contacto, número de serie del certificado digital …… (en caso de corresponder).

- **SOPORTE TÉCNICO DE FIRMA DIGITAL:**
  - **Nombre y APELLIDO**, tipo y número de documento de identidad, CUIL/CUIT, cuenta de correo institucional, teléfono laboral de contacto.

Asimismo, se solicita que los siguientes datos se asocien a la Aplicación de la Autoridad Certificante de la ONTI:

- **DOMINIOS DE CORREO ELECTRÓNICO:**
  - **ejemplo.gob.ar**
  - **ejemplo.gov.ar**

- **DOMICILIO NIVEL DE SEGURIDAD UNO:** (El/los domicilios declarados corresponden a las direcciones físicas dónde operarán los Oficiales de Registro, indicar los datos abajo consignados por cada domicilio a declarar)**:**
  - **Domicilio, Oficina y Piso, Localidad, Ciudad, Código Postal, Teléfono, e-mail de contacto institucional (ejemplo: firmadigital@xxxx.gob.ar).**

Sin otro particular, lo saludo atentamente. -

.....

Firma, Aclaración y DNI

(Responsable de la Autoridad de

Registro del Organismo)

A.1.3 Solicitud autorización AR móvil 2017 (Firmada por Máxima Autoridad)

……., ….. de …….. de ……

REF: SOLICITUD AUTORIZACIÓN –

CONFORMACIÓN AUTORIDAD DE REGISTRO MÓVIL.

AL RESPONSABLE DE LA AUTORIDAD CERTIFICANTE DE LA

OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN

S / D

Tengo el agrado de dirigirme a Ud. en relación a la Autoridad de Registro de la Autoridad Certificante ONTI en el Organismo ……., a fin de solicitarle autorización para incorporar la modalidad de trabajo en puesto móvil en el marco de la Política Única de Certificación de la AC-ONTI.

En tal sentido, y en virtud de la modalidad de trabajo en puesto móvil, se deja constancia que se ha cumplido con los requerimientos exigidos en el documento “Requerimientos para la conformación de Autoridades de Registro de la AC-ONTI”, como así también se ha tomado conocimiento del “Manual de Procedimientos de la AC-ONTI”, a los cuales asumimos el compromiso de cumplir conjuntamente con el marco normativo de Firma Digital.

Sin otro particular, saludo a usted atentamente.

.....

Firma, Aclaración y DNI

(Autoridad Máxima del Organismo Solicitante)

A.2 Posible modelo de Resolución

RESOLUCIÓN N° XXXX/XX

Viedma,

VISTO, la Ley N° 25.506, el Decreto N° 2628 del 19 de diciembre de 2002 y sus modificatorias de la entonces SECRETARÍA DE LA GESTIÓN PÚBLICA, la Disposición N° 11 del 30 de diciembre de 2014 de la JEFATURA DE GABINETE DE MINISTROS y la Resolución N° 37-E del 20 de diciembre de 2016 del MINISTERIO DE MODERNIZACIÓN.

CONSIDERANDO

Que la Ley Nacional N° 25.506 de Firma Digital, reconoce la eficacia jurídica del documento electrónico, la firma electrónica y la firma digital, estableciendo las características de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA.

Que el Decreto Nº 2628/02 y sus modificatorios, reglamentario de la ley antes citada, regula el empleo de la firma electrónica y la firma digital y su eficacia jurídica, asignando competencias a la Autoridad de Aplicación para establecer determinados actos y procedimientos.

Que el Art. 35°, del Decreto mencionado en el considerando anterior define: “Los Certificadores Licenciados podrán delegar en Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptores de certificados y de registro de las presentaciones y trámites que les sean formuladas, bajo la responsabilidad del Certificador Licenciado, cumpliendo las normas y procedimientos establecidos por la presente reglamentación”.

Qué, asimismo, el Art. 36° establece: “(...) Una Autoridad de Registro puede constituirse como una única unidad o con varias unidades dependientes jerárquicamente entre sí, pudiendo, delegar su operatoria en otras autoridades de registro, siempre que medie la aprobación del Certificador Licenciado (...)”.

Que la Oficina Nacional de Tecnologías de Información (ONTI) se adhirió a la Ley Nacional N° 25.506 de Firma Digital a través de la Disposición N° 11 del 30 de diciembre de 2014 de la JEFATURA DE GABINETE DE MINISTROS, en su calidad de Certificador Licenciado.

Que la UNIVERSIDAD NACIONAL DE RÍO NEGRO cuenta con sedes en diferentes zonas de la provincia de Río Negro y su delegación administrativa se encuentra localizada en la localidad de Viedma.

Que existe una necesidad de implementar el uso del Sistema de Firma Digital en toda la administración de la Universidad.

Que el Estatuto de la Universidad en su Art. 13° menciona la futura utilización de la firma digital con el fin de dotar de seguridad a las comunicaciones internas.

Que la presente se dicta en uso de las atribuciones conferidas por el Artículo 25º del Estatuto de la UNIVERSIDAD NACIONAL DE RÍO NEGRO.

Por ello,

EL RECTOR

DE LA UNIVERSIDAD NACIONAL DE RÍO NEGRO

RESUELVE

ARTÍCULO 1º.- Dar inicio a los trámites para conformar a la UNIVERSIDAD NACIONAL DE RÍO NEGRO como Autoridad de Registro de la Autoridad Certificante ONTI, con el fin de adherirse a la Ley nacional N.º 25.506, que regula la utilización del Sistema de Firma Digital, e implementarla en esta institución, en tanto no contradiga las normas dictadas en el marco de su autonomía.

ARTÍCULO 2º.- Designar como Responsables de Autoridad de Registro y Oficiales de Registro a los agentes que figuran en el Anexo X (crear anexo).

ARTÍCULO 3º.- Registrar, comunicar y archivar.