3C Tecnología ***(Edición 23)*** *Vol.6 – Nº 3*
Septiembre – diciembre'17, 14– 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

Recepción: 19 de abril de 2017
Aceptación: 6 de septiembre de 2017
Publicación: 14 de septiembre de 2017

ESTÁNDARES CRIPTOGRÁFICOS APLICADOS A LA INFRAESTRUCTURA DE CLAVE PÚBLICA DE AMÉRICA DEL SUR

CRYPTOGRAPHIC STANDARDS APPLIED TO THE PUBLIC KEY INFRAESTRUCTURE IN SOUTH AMERICA

José Antonio Carrillo Zenteno[1]
Aida Diana Ormaza Vintimilla[2]
Francisco Joseph Bolaños Burgos[3]

1. Catedrático y Coordinador del Departamento de Investigación de la Universidad Católica de Cuenca, extensión Cañar. Analista e Ingeniero de Sistemas, Magister en Sistemas de la Información Gerencial, (Ecuador). E-mail: jacarrilloz@ucacue.edu.ec
2. Analista e Ingeniero en Sistemas, Magister en Auditoría de Tecnologías de la Información, Universidad Espíritu Santo, (Ecuador). E-mail: aidaormaza@uees.edu.ec
3. Ingeniero en Computación, Especialización Sistemas de Información, Universidad Espíritu Santo, (Ecuador). E-mail: fcobolanos@uees.edu.ec

Citación sugerida:

Carrillo Zenteno, J.A., Ormaza Vintimilla, A.D. y Bolaños Burgos, F.J. (2017). Estándares criptográficos aplicados a la infraestructura de clave pública de América del Sur. *3C Tecnología: glosas de innovación aplicadas a la pyme*, 6(3), 14-32. DOI: <http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32/>.

3C Tecnología *(Edición 23)* Vol.6 – Nº 3
Septiembre – diciembre'17, 14– 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

RESUMEN

Una de las principales aplicaciones de la criptografía es la protección de la información, asegurando la autenticación, confidencialidad, la integridad de los datos, y el no repudio, utilidad que ha sido aprovechada para dotar a firmas y certificados digitales de seguridad, siendo necesario el empleo de la Infraestructura de Clave Pública como un modelo de confianza.

ABSTRACT

One of the main applications of cryptography is the protection of information, which ensures authentication, confidentiality, data integrity, and non-repudiation. This useful application has been used to provide security to signatures and digital certificates, being necessary the employment of Public-Key infrastructure as a reliable model.

PALABRAS CLAVE

Estándares criptográficos, FIPS 140-2, Common Criteria, PKCS, América del Sur.

KEY WORDS

Cryptographic standards, FIPS 140-2, Common Criteria, PKCS, South America.

3C Tecnología *(Edición 23)* Vol.6 – Nº 3
Septiembre – diciembre'17, 14– 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

1. INTRODUCCIÓN

Para Wollinger, Guajardo, & Paar (2003) la criptografía proporciona a los datos servicios de autenticación, confidencialidad, integridad y no repudio. Dichos servicios son procurados mediante diversos algoritmos criptográficos, siendo uno de ellos el de clave pública. Además, al ser la clave pública el algoritmo utilizado en las firmas digitales es fundamental que la distribución de claves públicas y certificados hagan uso de la Infraestructura de Clave Pública (ICP), con el propósito de generar confianza y certeza en los datos y mensajes transmitidos, así como también el contar con normas y estándares internacionales aceptados que brinden mayor seguridad.

Es así que el empleo de normativas y estándares internacionales proveen de los elementos suficientes para que la Infraestructura de Clave Pública sea segura, por lo que muchos países han adoptado diferentes estándares para firmas y certificados digitales. A pesar de conocer que los mismos son aplicados y requeridos para certificar la integridad de los datos, no se cuenta con información sobre cuál de ellos es el más utilizado en América del Sur.

Por esta razón, el presente trabajo pretende analizar información sobre los estándares criptográficos aplicados a la Infraestructura de Clave Pública a fin de determinar cuáles han sido adoptados por los diferentes países de América del Sur. Se ha realizado una revisión bibliográfica partiendo de conceptos básicos sobre: criptografía y criptología, certificados firma electrónica, firma digital, firma digital avanzada infraestructura de clave pública; continuando con la exposición de información sobre los estándares como FIPS, Common Criteria y PKCS, y por último, presentando los estándares exigidos en los diferentes países.

2. CRIPTOLOGÍA Y CRIPTOGRAFÍA

La Criptología es la ciencia que trata sobre la seguridad en el intercambio de mensajes entre el emisor y el receptor, etimológicamente viene del griego krypto y logos que significa estudio de lo oculto (Fernández, 2004) y comprende conjuntamente el estudio de la criptografía y del criptoanálisis (Álvarez Sánchez, 2005). Por su parte, la criptografía es la ciencia de la escritura secreta con el objetivo de ocultar el significado de un mensaje (Paar & Pelzl, 2010). Además, se encuentra relacionada con aspectos de seguridad de la información como: confidencialidad, integridad de datos, autenticidad y el no repudio (Castillo Rubí, M.A., Santana de la Cruz, Díaz Lobatón, Almanza Rodríguez, & Castillo Rubí, F., 2011).

La criptografía se divide en: criptografía simétrica y criptografía asimétrica. En cuanto a la criptografía simétrica o de clave privada, esta se caracteriza por utilizar una clave para cifrar y descifrar. Los métodos empleados para el cifrado simétrico utilizan operaciones matemáticas que pueden ser programadas en algoritmos de computación sencillos y extremadamente rápidos (Whitman & Mattord, 2012). Hay dos tipos de modos de cifrado de clave simétrica, uno es el cifrado de bloque y otro el cifrado de flujo; el primero funciona con grupos de bits llamados bloques, que son procesados varias veces, la clave aplicada es única en cada ronda y el segundo divide los datos tan pequeños como bits individuales, realizando el cifrado a continuación (Bisht & Singh, 2015).

3C Tecnología *(Edición 23)* Vol.6 – Nº 3
Septiembre – diciembre'17, 14– 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

Por otra parte, la criptografía asimétrica o de clave pública, utiliza dos claves diferentes, una pública que se distribuye libremente y que es empleada para cifrar y otra, denominada clave privada que es utilizada para descifrar (Marrero Travieso, 2003); de modo que cualquier mensaje (texto, archivos binarios o documentos) que es cifrado mediante la clave pública solo puede ser descifrado aplicando el mismo algoritmo, pero utilizando la clave privada coincidente (Rani & Kaur, 2017).

3. CERTIFICADOS

Whitman & Mattord (2012), indican que un certificado es un documento electrónico que contiene un valor clave e información de indentificación sobre la entidad que controla la clave y a menudo es emitido y certificado por un tercero denominado autoridad de certificación (AC). Así mismo y de acuerdo a lo expresado por Gentry (2003), además del usuario y la clave pública la AC incluye un número de serie SN, la fecha de emisión del certificado D1 y la fecha de vencimiento D2.

Un certificado permite enlazar de forma segura varias entidades, vincula a la persona o entidad (denominada entidad final) con su clave pública, una vez verificada que la entidad final posee realmente la clave pública particular la CA procede a asegurar el contenido del certificado a través de una firma digital a fin de evitar que éste sea alterado una vez emitido. Si un remitente quiere enviar un mensaje a un receptor, éste adjunta el certificado al mensaje, asegurándose de esta manera de la autenticidad de la clave pública (Balakrishnan, 2003).

4. FIRMA ELECTRÓNICA

Una firma electrónica es un mecanismo que permite identificar a una persona ante un sistema informático (Sistema Económico Latinoamericano y del Caribe, 2009). Son datos en forma electrónica depositados en un mensaje de datos, adjuntos o lógicamente asociados al mismo (Naciones Unidas, 2002), que puede acreditar quien es el firmante o emisor del mensaje (autenticación) y que además asegura que éste no ha sido manipulado o modificado por terceros en el transcurso de la comunicación (integridad) y da la seguridad de que el autor del mensaje no puede retractarse en el futuro de las acciones u opiniones dadas por él (Reyes, 2003).

5. FIRMA DIGITAL

Una firma digital es un análogo electrónico de una firma escrita (National Institute of Standards and Technology, 2013). Son datos consignados en un mensaje de forma electrónica o asociados al mismo, que pueden ser utilizados para identificar al firmante en relación con el mensaje de datos y que permiten determinar al firmante como dueño del mensaje (Naciones Unidas, 2002). Además, las firmas electrónicas generadas mediante criptografía asimétrica reciben el nombre de firma digital, por lo que la criptografía de clave pública o asimétrica es fundamental para proporcionar firmas electrónicas seguras (De Miguel Asensio, 2015), en el campo de las comunicaciones electrónicas (Velandia Ponce, 2011). Por lo tanto, el uso de la firma digital mediante el cifrado asimétrico, le provee al documento autenticación, satisfaciendo exigencias de autoría e integridad (Belloso Chacín, 2012).

3C Tecnología *(Edición 23)* Vol.6 – Nº 3
Septiembre – diciembre'17, 14– 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

6. FIRMA DIGITAL AVANZADA

Firma digital avanzada es aquella que se crea en un dispositivo seguro de firmas y que además se basa en un certificado calificado (Chondrocoukis & Lagou, s.f.). La tecnología de la firma digital avanzada utiliza un par de claves asimétrico: la clave privada y la clave pública. La clave privada debe permanecer en secreto mientras la clave pública es publicada y se utiliza para comprobar una firma digital y/o para enviar información confidencial en forma encriptada. Las claves privadas y públicas no pueden derivarse entre sí. Este par de claves es, en general, emitido por una autoridad de certificación que verifica y registra la identidad del firmante, pero también puede ser creada por el propio usuario. Al igual que el par de claves, el certificado digital puede ser creado por el propio remitente o por un intermediario autorizado como una autoridad de certificación que le proporciona un mayor grado de fiabilidad (Boudrez, 2005). Cabe mencionar que una firma digital avanzada debe cumplir con los siguientes requisitos: 1) Vinculada exclusivamente al signatario; 2) Capaz de identificar al firmante; 3) Creada utilizando medios que el firmante pueda tener bajo su control y 4) Estar vinculado a los datos de tal manera que cualquier cambio pueda ser detectado (Chondrocoukis & Lagou, s.f.).

7. INFRAESTRUCTURA DE CLAVE PÚBLICA

La infraestructura de clave pública es un conjunto de componentes que proporcionan seguridad completa en las comunicaciones digitales a través de redes privadas o públicas y que permite a los usuarios intercambiar datos de forma segura (Sumalatha & Sathyanarayana, 2015). Según Chaparro, Greenwood, & Barán (2008), la infraestructura de clave pública es un medio que facilita el acceso a las claves públicas que asegura la correspondencia unívoca entre las claves públicas y sus respectivos usuarios. La ICP – PKI es necesaria para crear, manejar, almacenar, distribuir y revocar certificados digitales basados en criptografía asimétrica (Solinas et al., 2013). Además, proporciona seguridad y confianza, así como también el software, hardware, políticas y mecanismos de seguridad que garanticen las operaciones criptográficas como el cifrado, la firma digital y el no repudio (Boiero & Tapia, 2014).

De acuerdo con RSA Data Security (1999), los tres componentes funcionales de la Infraestructura de Clave Pública son: 1) La Autoridad de Certificación AC, es la entidad que emite los certificados; 2) el Repositorio de Claves, Certificados y Listas de Revocación de Certificados LRC – CRL que suelen basarse en un protocolo de servicio de acceso a Directorio (LDAP); 3) Autoridad de Registro AR la misma que se dedica al registro de usuarios a través de un proceso de recolección de información y verificación de la identidad del mismo para registrar un usuario de acuerdo con una política y la aceptación de solicitudes de certificados; 4) Partes de confianza, que son los organizaciones y/o individuos que confían en el certificado para usar la clave pública dentro de ese certificado y 5) Repositorios que son las organizaciones y/o entidades que permiten publicar, almacenar y tener acceso a certificados y otra información relacionada con la ICP – PKI (American Bar Association, 2003). Por otro lado, la ICP –PKI tiene algunas funciones (ver tabla 1).

3C Tecnología (Edición 23) Vol.6 – Nº 3
Septiembre – diciembre'17, 14– 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

Funciones	Descripción
Registro de usuarios	Recopila y verifica la información del usuario.
Emisión de certificados	Crea certificados en respuesta a la solicitud de un usuario o administrador.
Revocación de certificados	Crea y publica listas de revocación de certificados LRC
Almacenamiento y recuperación	Elaborar certificados y LRCs para usuarios autorizados
Certificado basado en políticas	Imponer restricciones basadas en políticas en la cadena de validación de rutas de certificados y validar el cumplimiento de las restricciones.
Sellar el certificado	Establecer un tiempo de validez, combinando firmas digitales con sellos de tiempo
Gestión de ciclo de vida de la clave	Actualizar, archivar y restaurar claves

Tabla 1. Funciones de la ICP – PKI Fuente: Página RSA Security.
Elaboración: adaptación de RSA Security.

8. ESTÁNDARES CRIPTOGRÁFICOS

En el ámbito de la criptografía, los estándares criptográficos se definen como modelos, normas o referencias que aseguran la transmisión de información privada. Esta estandarización se consigue por la revisión continua que realizan ciertos organismos y laboratorios a los diferentes algoritmos de cifrado, a la seguridad de las claves y a su durabilidad, con el objetivo de contar con procedimientos seguros, confiables y resistentes ante diferentes tipos de ataques. La certificación del sistema de cifrado debe estar otorgada por un Organismo de Certificación competente en materia de seguridad (Rodríguez Cabrero, 2007). Prueba de ello es el Instituto Nacional de Normas y Tecnologías (National Institute of Standars and Technology) ubicado en los Estados Unidos, que constantemente realiza un proceso de prueba y filtrado de los nuevos algoritmos, y los incorpora a una lista de nuevos métodos criptográficos aprobados.

9. COMMON CRITERIA

Según Eterovic & Donadello (2014), Common Criteria (CC) define un criterio estándar que se usa como base para la evaluación de las propiedades y características de un determinado producto o sistema de Tecnologías de Información. American Bar Association (2003), señala que CC es un catálogo de requisitos de seguridad con dependencias indicadas. Se dan requisitos para las características de seguridad y para el aseguramiento de seguridad. Los requerimientos funcionales son proporcionados para las siguientes áreas: Auditoría, no repudio, características criptográficas generales, protección de datos de usuario, identificación y autenticación, gestión de la funcionalidad de seguridad, intimidad, protección de las funciones de seguridad y sus datos, uso de recursos, control de acceso al objetivo de evaluación (TOE), entre otros.

Por otro lado, en lo que se refiere a la ICP – PKI, CC no evalúa cuestiones de personal, procedimientos u otras cuestiones no técnicas. Su evaluación tiene tres actores principales: 1) Esquema, es el encargado de supervisar la evaluación, emitir la aprobación para que el evaluador realice la evaluación

3C Tecnología *(Edición 23)* Vol.6 – Nº 3
Septiembre – diciembre'17, 14– 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

y confirmar los resultados de la misma; 2) Patrocinador, persona u organización que contrata el laboratorio de evaluación y 3) El laboratorio, aprobado por el sistema nacional que certifique que ésta cumple con un requisito identificado y se coloca en la lista nacional de productos evaluados (American Bar Association, 2003).

9.1. ELEMENTOS COMMON CRITERIA

- **PERFIL DE PROTECCIÓN - PP**

Documento formal que expresa un conjunto de requisitos a los que debe ajustarse un producto TI con la finalidad de asegurar que su funcionamiento es correcto y que cumple con las necesidades específicas de los clientes (INTECO, s.f.). Además, puede ser empleado como base para establecer requisitos encaminados a definir un Objetivo de Seguridad ST (Eterovic & Donadello, 2014).

- **OBJETIVO DE SEGURIDAD - ST**

Es el seguimiento lógico de un PP, puede ser también el punto de partida para la captura de un diseño existente en la construcción CC. Proporciona una estructura común para expresar las capacidades de seguridad, mejorando la capacidad de la comunidad de usuarios para interpretar reclamos de proveedores. Provee de los mecanismos necesarios para para que los reclamos de los proveedores puedan ser fácilmente evaluados por terceros (American Bar Association, 2003).

- **REQUISITOS FUNCIONALES SE SEGURIDAD - SFR**

Los SFR forman una descripción clara, inequívoca y bien definida del comportamiento de seguridad esperado del objetivo de la evaluación TOE (Common Criteria, 2012). Los SFR se encuentran en un nivel de abstracción más detallado, en el que los objetivos de seguridad deben ser abordados completamente y ser independientes de cualquier solución técnica específica (Common Criteria, 2017). Los propósitos de SFR son: 1) describir el comportamiento de seguridad de un TOE; 2) alcanzar los objetivos de seguridad establecidos en el PP o en el ST; 3) anular las amenazas en el entorno del TOE; 4) cumplir las políticas de seguridad reconocidas por la organización y 5) especificar las propiedades de seguridad que los usuarios pueden detectar directamente o respondiendo a un estímulo (INTECO, s.f.).

- **OBJETIVO DE EVALUACIÓN - TOE**

Producto o sistema de tecnología de la información que se va a evaluar acompañado de las guías de uso, para el cual se especifican requisitos de seguridad en un perfil de protección o en un objetivo de seguridad (American Bar Association, 2003); es la implementación física del ST (INTECO, s.f.).

3C Tecnología ***(Edición 23)*** *Vol.6 – Nº 3*
Septiembre – diciembre'17, 14 – 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

- **REQUISITOS DE ASEGURAMIENTO DE LA CALIDAD - SAR**

Requisito de garantía que define como se evaluará TOE, PP y ST. Permite comparar dos ST dado que los diferentes autores del ST pueden utilizar una terminología diferente para describir la evaluación, el lenguaje estandarizado ya que se aplica la misma tecnología y conceptos; así mismo proporciona una descripción exacta de cómo se evaluará TOE (Common Criteria, 2017).

- **NIVEL DE ASEGURAMIENTO - EAL**

De acuerdo a Common Criteria (2012), el nivel de aseguramiento de evaluación NAE – EAL se utiliza para determinarla implementación de los requisitos de seguridad para un producto o grupo de productos específicos, tiene siete niveles ordenados jerárquicamente, descritos a continuación:

- **EAL.1. PROBADO FUNCIONALMENTE**

Este nivel es aplicable cuando se requiere un nivel básico de aseguramiento, donde las amenazas a la seguridad no son consideradas como graves proporciona evidencia de que las funciones de Seguridad de los Objetivos de Evaluación (TOE **Target of Evaluation**) se encuentran implementadas de manera consistente y que propocionan una protección adecuada contra las amenazas.

- **EAL.2. PROBADO ESTRUCTURALMENTE**

Exige el cumplimiento de los requisitos del nivel anterior, siendo necesario haber realizado un análisis completo de los Requisitos Funcionales de Seguridad (SFR Security Funcional Requisites) en el objetivo de seguridad (ST **Security Target)**. El análisis se apoya en pruebas independientes de la Evaluación de Tecnologías de Seguridad (TSF) evidencia de las especificaciones, confirmación independiente de esas pruebas y un análisis de vulnerabilidad que demuestre resistencia a ataques básicos. Es necesaria la cooperación del equipo de desarrollo para que se entregue la información sobre diseño y pruebas de testing.

- **EAL.3. PROBADO Y COMPROBADO METODOLÓGICAMENTE**

Permite a los desarrolladores la máxima garantía de seguridad en la etapa de diseño, añade al nivel anterior el uso de controles de seguridad en el proceso de desarrollo para garantizar que el producto no ha sido manipulado y representa un aumento significativo con relación al nivel anterior.

- **EAL. 4. DISEÑADO, PROBADO Y REVISADO METODOLÓGICAMENTE**

Permite a un desarrollador obtener la máxima garantía basado en las buenas prácticas de desarrollo comercial y no requiere un conocimiento especializado, habilidades y otros recursos. Necesita de un análisis de vulnerabilidades independiente, demostrando resistencia a intrusos con bajo potencial de ataque. Representa un aumento significativo en la garantía de EAL3.

- **EAL.5. DISEÑADO Y PROBADO SEMIFORMALMENTE**

Es aplicable en aquellos casos en que los desarrolladores o usuarios requieren un alto nivel de seguridad. El análisis se apoya en pruebas independientes del TSF, evidencia de las pruebas basadas en la especificación funcional, diseño del TOE, confirmación selectiva independiente del resultado de las pruebas, análisis de vulnerabilidad independiente contra ataques moderados, proporciona garantía en el desarrollo de controles de medio ambiente y gestión de la configuración incluyendo

3C Tecnología ***(Edición 23)*** *Vol.6 – Nº 3*
Septiembre – diciembre'17, 14 – 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

automatización y evidencia de entrega de procedimientos de seguro. Representa un aumento significativo en la garantía de EAL4.

- **EAL. 6. DISEÑADO, PROBADO Y VERIFICADO SEMIFORMALMENTE**

Permite a los desarrolladores obtener un alto grado de aseguramiento en un entorno de desarrollo riguroso con el fin de producir un TOE para protección de los activos de valor contra riesgos significativos, donde el valor de los bienes protegidos justifica los costes adicionales. Este nivel representa un avance importante en relación al nivel EAL 6, pues requiere un análisis más exhaustivo, una representación estructurada de la ejecución, mejor estructura arquitectónica, un análisis independiente de vulnerabilidades más amplio y mejorado, controles de gestión de la configuración y el entorno de desarrollo.

- **EAL. 7. NIVEL DE GARANTÍA DE EVALUACIÓN VERIFICA Y PRUEBA FORMALMENTE EL DISEÑO**

Se aplica al desarrollo de TOE de seguridad para su adaptación en situaciones de alto riesgo y/o donde el valor de los activos justifica los costos altos. Necesita de un análisis más exhaustivo utilizando representaciones formales y pruebas completas.

10. FIPS 140-2

Estándar de Procesamiento de Información Federal es un conjunto de normas que especifican los requerimientos de seguridad para módulos criptográficos; el cual es aplicable a las agencias federales que utilizan sistemas de seguridad basados en criptografía para proteger la información sensible en los sistemas informáticos y de telecomunicaciones. De la misma forma, este estándar proporciona protección a la información asegurando la confidencialidad e integridad de los datos. FIPS 140-2 reemplazó a FIPS 140-1 debido a los cambios en lo que ha tecnología y prácticas se refiere (Kenworthy, 2002). Además, esta norma proporciona cuatro niveles de seguridad: Nivel 1, Nivel 2, Nivel 3 y Nivel 4; éstos incluyen la especificación de módulos criptográficos, puertos e interfaces de módulos criptográficos, funciones, servicios y autenticación, seguridad física y gestión de claves criptográficas. Los cuatro niveles de seguridad se especifican a continuación (National Institute of Standards and Technology, 2001).

- **NIVEL 1**

Es el nivel de menor exigencia, y en él se definen requisitos de seguridad básicos para un módulo criptográfico. No se requieren mecanismos específicos de seguridad física, por lo que esta implementación es apropiada cuando los niveles de seguridad física no existen o son inapropiados.

- **NIVEL 2**

Mejora mecanismos de seguridad física en un nivel criptográfico. Requiere autentificación basada en roles y el módulo criptográfico debe verificar la autorización de un operador para tener acceso a un conjunto específico de servicios. Por lo tanto, en este nivel los componentes de software y firmware de un sistema operativo deben haber sido evaluados con un nivel EAL2 o superior de Common Criteria.

3C Tecnología *(Edición 23)* Vol.6 – Nº 3
Septiembre – diciembre'17, 14 – 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

- **NIVEL 3**

Incorpora mecanismos de detección de intrusos, evitando el acceso no autorizado, uso o modificación de los módulos criptográficos. Además, se incluye protección criptográfica eficaz y administración de claves que se requieren para la autenticación. También, el software y firmware de un sistema operativo debe haber sido evaluado con un nivel EAL3 o superior.

- **NIVEL 4**

Contiene las mayores exigencias de seguridad y protección alrededor de un módulo criptográfico. Este nivel de seguridad es útil para el funcionamiento en entornos físicamente sin protección.

11. ESTÁNDAR PKCS

Son estándares de criptografía de clave pública, ofrecidos por los laboratorios de RSA[1], cuyo objetivo es facilitar el uso de tecnologías de clave pública (Ortiz Figueroa, 2010). Según Wang (2012), este estándar tiene el propósito de acelerar el despliegue de la criptografía de clave pública. Además, PKCS define también una sintaxis de algoritmo independiente para firmas digitales, sobres digitales y certificados extendidos. La tabla 1 muestra el detalle del estándar criptográfico de clave pública (RSA Laboratories, 2015).

Niveles	Características
PKCS#1	Define los mecanismos para la encriptación de datos y firma utilizando el sistema de cifrado de clave pública RSA.
PKCS#3	Define un protocolo de acuerdo de claves Diffie-Hellman.
PKCS#5	Describe un método para cifrar una cadena con una clave secreta derivada de una contraseña.
PKCS#6	Se está eliminando a favor de la versión 3 de X.509.
PKCS#7	Define una sintaxis general para los mensajes que incluyen mejoras criptográficas, como las firmas digitales y cifrado.
PKCS#8	Describe un formato de información de clave privada. Esta información incluye una clave privada para algún algoritmo de clave pública, y, opcionalmente, un conjunto de atributos.
PKCS#9	Define seleccionado tipos de atributos para su uso en los otros estándares PKCS.
PKCS#10	Describe la sintaxis para las solicitudes de certificación.
PKCS#11	Define una interfaz de programación independiente de la tecnología, llamada Cryptoki, para dispositivos criptográficos como tarjetas inteligentes y tarjetas PCMCIA.
PKCS#12	Especifica un formato portátil para almacenar o transportar las claves de un usuario privado, certificados, secretos diversos, etc.

[1] Rivest, Shamir y Adleman. Sistema criptográfico de clave pública

3C Tecnología *(Edición 23)* Vol.6 – Nº 3
Septiembre – diciembre'17, 14 – 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

PKCS#13	Tiene por objeto definir los mecanismos para el cifrado de datos y firma utilizando criptografía de curva elíptica.
PKCS#14	Está actualmente en desarrollo y cubre la generación de números pseudo-aleatorios.
PKCS#15	Es un complemento de PKCS # 11 que da un estándar para el formato de las credenciales criptográficas almacenadas en tokens criptográficos.

Tabla 2. Niveles del Estándar PKCS.
Fuente: Página RSA Laboratories.
Elaboración: los autores.

12. ESTÁNDARES APLICADOS A MÓDULOS CRIPTOGRÁFICOS EN FIRMA Y CERTIFICADOS DIGITALES EN LOS PAISES DE AMÉRICA DEL SUR

12.1. ARGENTINA

La firma digital en la República de Argentina se encuentra reglamentada en la ley 25.506, sancionada el 14 de noviembre de 2001, promulgada el 11 de diciembre de 2011 y publicada el 14 de diciembre de ese mismo año (Ventura, s.f.). En la actualidad, la Firma Digital cuenta con una Entidad Certificante Raíz, administrada por la oficina de Tecnologías de Información. Así mismo, las firmas digitales al constituirse en una aplicación muy importante de la tecnología de claves públicas, deben apoyarse en estándares tecnológicos. Sus componentes son: 1) estándares para algoritmos de encriptación y algoritmos hash, 2) protocolos para facilitar el acceso de los usuarios a las claves públicas, 3) Estándares para la generación segura de pares de claves, entre otros (Rivolta, 2010).

En lo que se refiere a los estándares tecnológicos, la autoridad encargada es la Jefatura de Gabinete de Ministros, quienes pueden determinar los estándares internacionales que se utilizarán. El estándar reconocido es el X.509 versión 3, estándar que fue adoptado porque vincula la clave pública con los datos de identificación del titular (Ventura, s.f.).

Según Guini (2011), solo aquellas firmas aprobadas o licenciadas por Autoridad de Aplicación podrán demostrar la validez de la firma electrónica, el estándar criptográfico utilizado es FIPS 140-2 nivel 3 para dispositivos seguros en la creación de la firma y para dispositivos de almacenamiento de respaldo en un sitio de contingencia.

12.2. BRASIL

En Brasil la firma digital se promulgó en la Medida Provisória Nº 2.200-2, de 24 de Agosto de 2001 Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, e dá outras providências (Pario Communications Limited, 2013). Al mismo tiempo, la firma digital en Brasil se basa en la infraestructura de clave pública (ICP – Brasil), que debe ser emitida por autoridad certificada

3C Tecnología ***(Edición 23)*** *Vol.6 – Nº 3*
Septiembre – diciembre'17, 14 – 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

autorizada y de conformidad a los estándares y normas establecidos (Lopes Campos, Campos Zaghloul, & Zanforlin Pereira, 2014).

Según Magioli Nuñez (2013), la autoridad responsable de la infraestructura de clave pública es el Instituto de tecnología de Brasil (ITI), que se constituye en la autoridad de certificación raíz, es la encargada de realizar las políticas y directrices de los certificados. En cuanto a los parámetros de generación de claves asimétricas, módulos criptográficos y parámetros de generación de claves, de acuerdo al documento de clave pública (DOC – ICP_01.01. Versão 2.6), en Brasil se adoptarán los estándares FIPS 140-1 o su equivalente, FIPS 140-1 nivel 2 (para la cadena de certificados V0); o FIPS 140-2 Nivel 2 (para la cadena V1 de acreditación); o FIPS 140-2 nivel 3 (para la cadena de certificados V2 y V3) utilizando el algoritmo ECDSA[2] o RSA (Instituto Nacional de Tecnologia da Informação).

12.3. BOLIVIA

De acuerdo a Red Iberoamericana de Protección de datos (2013), en Bolivia la firma digital se encuentra reglamentada en la Ley Nro. 164 del 8 de agosto de 2011 que corresponde a la Ley general de Telecomunicaciones, Tecnologías de Información y Comunicación sobre desarrollo, contenidos y aplicaciones de tecnología de información y comunicación; en la que se establece la normativa que deberán cumplir las entidades certificadoras autorizadas para la emisión de certificados digitales, mismos que deberán responder a los formatos y estándares internacionales reconocidos por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT). Las entidades certificadoras deberán establecer los formatos y procedimientos necesarios para la aplicación de la firma digital y los certificados digitales, los cuales se basarán en el estándar internacional RFC5280 en el cual se definen los formatos de certificados X.509 versión 3 (González Cruz, 2005) y los CRL (lista de certificados revocados) X.509 versión2. Además, el estándar FIPS 140-2 para el almacenamiento y custodio del certificado digital y su clave privada (Autoridad de regulación y fiscalización de telecomunicaciones y transportes, 2014).

12.4. CHILE

Según, Formentín Zayas (2013), la Ley 19.799 de 2002 corresponde a la Ley sobre Firma electrónica en Chile, promulgada el 26 de marzo de 2002. En cuanto a los tipos de firma electrónica, existen dos la simple y la avanzada (Quintanilla, Doren, & Hernández, 2014). En Chile la firma digital avanzada es aquella que permite firmar documentos, otorgándoles validez legal, certificada por un prestador acreditado y que emplea la infraestructura de clave pública (PKI), diferenciándola de esta manera de la firma digital simple. Es así que, la firma digital avanzada cumple con exigentes estándares de seguridad, con la participación de entidades altamente tecnificadas y calificadas (Fernández Acevedo, 2004). Al mismo tiempo, la Subsecretaría de Economía cumple como entidad certificadora de modo que para que todos los certificados de los documentos firmados con firma electrónica avanzada sean válidos deberán pasar por el proceso de acreditación oficial de la Subsecretaría de Economía (Ministerio Secretaría General de la Presidencia. Proyecto Reforma y Modernización del Estado, 2013).

Según el Ministerio de Economía, Fomento y Turismo del Gobierno de Chile (2013), la certificación de la firma digital avanzada debe contar con el estándar internacional FIPS 140- 2 nivel 2 para la

[2] Algoritmo de firma digital de curva elíptica

3C Tecnología ***(Edición 23)*** *Vol.6 – Nº 3*
Septiembre – diciembre'17, 14 – 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

implementación o administración de llaves criptográficas y para verificar el nivel de seguridad del dispositivo seguro de los usuarios, el estándar FIPS 140-2 nivel 2 (o Common Criteria EAL 3).

12.5. COLOMBIA

Según Rojas López, Suarez Botero, & Meneses Durango (2011), la ley sobre firma digital es la Ley 527 de 1999 que tomó como base la Ley modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional CNUDMI promulgada por las Naciones Unidas y adaptada a la jurisprudencia colombiana, cuyo ámbito de aplicación es el uso de firmas digitales en los mensajes de datos. En Colombia, la supervisión de la infraestructura de clave pública está a cargo de la Superintendencia de Industria y Comercio, que concede la licencia para conformar entidades de certificación, las que para obtener licencia de funcionamiento deben estar alineados con la norma ISO o los estándares ITU reconocidos por el ende gubernamental (Salazar, 2009).

Por otro lado, la Organismo Nacional de Acreditación de Colombia establece criterios específicos para la acreditación de entidades de certificación digital de acuerdo a lo establecido en la Ley 527, Anexo F en lo que se refiere a Dispositivos Criptográficos, el cual especifica que los dispositivos criptográficos para el almacenamiento de certificados digitales y llave privada de los suscriptores debe cumplir con el certificado FIPS 140-2 nivel 3 o superior, o longitud de clave RSA 2048 o superior. Así también, los dispositivos criptográficos deberán cumplir con el certificado FIPS 140-2 nivel 3, RSA 2048 o superior, exigible 4096 cuando se declare inseguro RSA 2048 (Organismo Nacional de Acreditación de Colombia, 2014).

12.6. ECUADOR

En el Ecuador, la firma electrónica tuvo sus inicios en el año 2002 a través de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, teniendo igual validez que una firma manuscrita. La entidad de certificación de la firma electrónica es el Consejo Nacional de Telecomunicaciones[3].

La generación del par de claves de las Autoridad de Certificación Raíz y Subordinada, se generan con módulos criptográficos Hardware Security Module PKCS#11 y cumple con los requisitos establecidos para la protección de dispositivos seguros para la Autoridad de Certificación de acuerdo con Common Criteria y FIPS 140-2 nivel 3 o un nivel superior de seguridad. Para el almacenamiento de la clave en el token se utilizará FIPS 140-2 nivel 2 o nivel 3 y, para los certificados emitidos en dispositivos criptográficos se aplicará el estándar FIPS 1 nivel 2 o superior (Banco Central del Ecuador, 2013).

12.7. PARAGUAY

La firma digital en Paraguay fue reglamentada en la Ley Nro. 4017/10, de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico, a través del decreto Nro. 7.369 (Secretaría permanente del SELA, 2012). El Ministerio de Industrias y Comercio (MIC), por medio de la Subsecretaría de Estado de comercio es la autoridad de aplicación que tiene a su cargo la política de certificación, cuyo cumplimiento es de carácter obligatorio, los controles y medidas de seguridad tomados para proteger las claves criptográficas y datos de activación. Además, las claves

[3] Actualmente conocida con el nombre de Agencia de Control y Regulación de las Telecomunicaciones

3C Tecnología (Edición 23) Vol.6 – Nº 3
Septiembre – diciembre'17, 14 – 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

privadas de las autoridades certificadoras de firma digital deben cumplir como mínimo con el estándar FIPS 140-2 nivel 3 para el caso de módulos criptográficos, certificados de persona jurídica para firma digital y generación de claves. Para certificados de personas físicas para firma digital se aplicará el estándar FIPS 140-2 nivel 2 (Ministerio de Industria y Comercio. Subsecretaría de Estado de Comercio de la República de Paraguay).

12.8. PERÚ

El 26 de mayo de 2000 se promulgó en Perú la Ley 27.269 de firmas y certificados digitales, cuyo principal objetivo es el de regular el uso de la firma electrónica en sus dos modalidades: electrónica y digital (Mendoza Navarro, 2007). De acuerdo a esta ley la firma digital es una firma electrónica que utiliza criptografía asimétrica, generada a partir de certificados digitales, emitidos por entidades de certificación aprobados (Ministerio de Justicia del Perú).

El Instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual, es la autoridad administrativa competente encargada de la regulación de la estructura de la firma digital. A través del documento de Lineamientos de la política de la Infraestructura Oficial de la Firma Digital (IOFD), establece que para los procesos criptográficos con dispositivos certificados se empleará como nivel mínimo el estándar FIPS 140-1 Nivel 3 o Common Criteria EAL4 u otro equivalente que facilite el reconocimiento trasnacional de los certificados (INDECOPI, 2006). Además, la entidad encargada para emitir certificados raíz para las entidades de certificación del estado Peruano y proponer las políticas y estándares para las entidades de certificación y entidades de registro y verificación es el Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), que utiliza los siguientes estándares como parte de los controles del módulo ciptográfico: FIPS 140-2 Nivel 3 y Common Criteria EAL4+ (Registro Nacional de identifiación y estado civil, 2013).

12.9. URUGUAY

La firma electrónica en Uruguay está regulada por la Ley 18.600 aprobada el 21 de septiembre 2009 y publicada el 5 de noviembre del mismo año. En ésta se reconoce la validez de la firma electrónica y se instituye la diferencia entre la simple y la avanzada, estableciendo que la avanzada es creada con un dispositivo de creación de firmas y emitida por un prestador de servicios certificado acreditado. El lanzamiento de la infraestructura de claves públicas se realizó en el año 2011. La entidad certificadora es la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC), que depende directamente de la Presidencia de la República (Bouvier Villa, Cami Soria, & Ferreira Pina, 2012). Asimismo, se ha autorizado a la Administración Nacional de Correos (ANC) la generación de claves, generación y revocación de certificados y archivos de certificados emitidos. En cuanto a los estándares que se aplicarán a los módulos criptográficos y a la generación del par de claves éstos deben estar de acuerdo con la ITSEC[4], FIPS 140-1, Nivel 3 o Common Criteria (Correo Uruguayo, 2011) .

12.10. VENEZUELA

[4] Information Technology Security Evaluation Criteria

3C Tecnología (Edición 23) Vol.6 – Nº 3
Septiembre – diciembre'17, 14 – 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

De acuerdo a Arias Ferrer (2008), la Ley sobre Mensajes de Datos y Firmas Electrónicas (LMDFE) fue publicado 28 de febrero de 2001, en el que una firma digital es aquella que utiliza un certificado emitido por un Proveedor de Servicios de Certificación. Según Arcila & De la Barra (2009), la firma electrónica puede sustituir a una firma autógrafa siempre que ésta tenga el debido certificado de autenticidad, mismo que debe ser expedido por un proveedor registrado, que de acuerdo a la Ley sobre mensajes de Datos y Firmas Electrónicas, el ente que supervisa a los proveedores de servicios de certificación es la Superintendencia de Servicios de Certificación Electrónica.

De igual forma, la norma nro. 040, de la Guía de Estándares Tecnológicos y Lineamientos de seguridad para la Acreditación y revocación como proveedor de servicios de certificación o casos especiales, en la sección donde se referencia el plan de administración de claves públicas, señala que los estándares de evaluación que se aplicarán son ETSI TS 102 042[5] y FIPS 140-2 (SUSCERTE, 2012).

13. CONCLUSIONES

De acuerdo a la información recolectada durante el desarrollo de este trabajo se ha podido determinar que el estándar más utilizado para garantizar seguridad es el estándar FIPS 140-2 Nivel 1, Nivel 2 y Nivel 3.

Sin embargo, a pesar de que los estándares criptográficos han sido asumidos por los países de América del Sur, no se dispone de suficiente información procedente de otros autores que puedan ofrecer referencias sobre los estándares empleados en módulos y claves criptográficas.

Finalmente, sería importante realizar una revisión con mayor detalle sobre las características y el funcionamiento de FIPS 140-2, toda vez que éste estándar es el más utilizado para validar módulos criptográficos y que debido al objetivo de este trabajo no pudo ser abordado, dejando su desarrollo para trabajos futuros.

[5] Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates

3C Tecnología ***(Edición 23)*** *Vol.6 – Nº 3*
Septiembre – diciembre'17, 14 – 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

14. REFERENCIAS BIBLIOGRÁFICAS

Álvarez Sánchez, R. I. (2005). Universidad de Alicante. Obtenido de http://rua.ua.es/dspace/bitstream/10045/13571/1/tesis_ralvarez.pdf

American Bar Association. (2003). Recuperado el 23 de Agosto de 2017, de https://www.americanbar.org/content/dam/aba/events/science_technology/2013/pki_guidelines.authcheckdam.pdf

Arcila, C., & De la Barra, R. (2009). Aspectos legales del gobierno electrónico en Venezuela. Disertaciones, 238-259.

Arias Ferrer, M. I. (2008). La Ley sobre Mensajes de Datos y Firma Electrónica. Comentarios a la Sentencia de fecha 12 de febrero de 2008. Scielo , 177-190.

Autoridad de regulación y fiscalización de telecomunicaciones y transportes. (11 de Julio de 2014). ATT. Obtenido de http://att.gob.bo/

Balakrishnan, T. (2003). *Universidad de Leeds.* Recuperado el 20 de Agosto de 2017, de https://minerva.leeds.ac.uk/

Banco Central del Ecuador. (Noviembre de 2013). Banco Central del Ecuador. Obtenido de https://www.eci.bce.ec

Barberán, C. F., Barberán, L. A., Bontempo, V., Lens, S. A., Pérez Williams, A., & Scattolin, A. (s.f.). HfernandezdelPech. Recuperado el 21 de Octubre de 2015, de http://www.hfernandezdelpech.com.ar/PUBLICAtrabajosFirmaDigital.htm

Belloso Chacín, R. (2012). El documento electrónico, contratación electrónica y firma electrónica en el ordenamiento jurídico de la República Bolivariana de Venezuela. Revista Electrónica de Estudios Telemáticos, 33-49.

Bisht, N., & Singh, S. (2015). A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms. *International Journal of Innovative Research in Science, Engineering and Technology*, 1028-1031.

Boudrez, F. (2005). Recuperado el 2 de Septiembre de 2017, de http://www.edavid.be/docs/digitalsignatures.pdf

Boiero, F., & Tapia, C. (2014). Fortalecimiendo de la seguridad de las comunicaciones mediante la implementación de una infraestructura de clave pública. Cytal, 339-344.

Bouvier Villa, E., Cami Soria, G., & Ferreira Pina, J. (2012). Asociación de Escribanos de Uruguay. Obtenido de www.aeu.org.uy/andocasociado.aspx?2680,8152

Castillo Rubí, M. A., Santana de la Cruz, N., Díaz Lobatón, A. M., Almanza Rodríguez, G., & Castillo Rubí, F. (2011). Teoría de números en criptografía y su debilidad ante la posible era de las computadoras cuánticas. Ciencia Ergo Sum, 264-273.

Chaparro , R., Greenwood, P., & Barán, B. (2008). Alternativa de Infraestructura de Clave Pública Basada en el Uso de DNSSEC. Centro Latinoamericano de estdudios informáticos. Obtenido de http://clei.org/clei2004/HTML/PDFS/188.PDF

Common Criteria. (Septiembre de 2012). Common Criteria. Obtenido de https://www.commoncriteriaportal.org

3C Tecnología ***(Edición 23)*** *Vol.6 – Nº 3*
Septiembre – diciembre'17, 14 – 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

Common Criteria. (2017). *Common Criteria.* Recuperado el 01 de Septiembre de 2017, de http://www.commoncriteriaportal.org

Correo Uruguayo. (12 de Abril de 2011). Correo Uruguayo. Obtenido de www.correo.com.uy/correocert/cps.pd

Chondrocoukis, G., & Lagou, P. (s.f. de s.f. de s.f.). *semanticscholar.* Recuperado el 2 de Septiembre de 2017, de https://pdfs.semanticscholar.org/4c5f/a8a560251f3aa4ab29a34fa904f2c5120669.pdf

De Miguel Asensio, P. A. (15 de Octubre de 2015). eprints.ucm.es. Obtenido de http://eprints.ucm.es/6867/1/Direitosocinffirmelectr19.03.03.pdf

Eterovic, J. E., & Donadello, D. (15 de Enero de 2014). Ciencia y Técnica Administrativa. Obtenido de http://www.cyta.com.ar/ta1301/v13n1a4.htm

Fernández Acevedo, F. (2004). scielo. Obtenido de http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122004000200005&lang=en

Formentín Zayas, Y. M. (Enero de 2013). La firma electrónica, su recepción legal. Especial referencia a la ausencia legislativa en Cuba. Revista del Instituto de Ciencias Jurídicas de Puebla, 104-120.

Gentry, C. (13 de Mayo de 2003). Certificate-Based Encryption and the Certificate Revocation Problem. *International Conference on the Theory and Applications of Cryptographic Techniques*, (págs. 272-293).

González Cruz, R. (Agosto de 2005). Universidad San Francisco Javier. Obtenido de www.criptored.upm.es/guiateoria/gt_m115a.htm

Guini, L. (2011). Validez probatoria de firma electrónica emitida por un certificador no licenciado dentro de la infraestructura de firma digital en Argentina. Revista Digital ElDerechoInformático.

INDECOPI. (31 de Agosto de 2006). INDECOPI. Obtenido de http://www.iofesac.com/noticias/Implementaci%C3%B3n_IOFE_INDECOPI.pdf

Information Technology Laboratory National Institute of Standards and Technology. (25 de Mayo de 2001). National and Institute of Standards and Technology. Obtenido de http://csrc.nist.gov/

Instituto Nacional de Tecnologia da Informação. (s.f.). Instituto Nacional de Tecnologia da Informação. Obtenido de www.iti.gov.br

Kenworthy, T. (30 de Julio de 2002). SANS Institute. Obtenido de https://www.sans.org

Lopes Campos, R., Campos Zaghloul, B., & Zanforlin Pereira, L. H. (25-27 de Marzo de 2014). VII Congresso CONSAD de gestão Pública . Governo Sem Papel: Desenvolvendo a cultura. Brasilia, Brasil. Obtenido de http://banco.consad.org.br/bitstream/123456789/1105/1/C7_PP_GOVERNO%20SEM%20PAPEL%20DESENVOLVENDO%20A%20CULTURA.pdf

Magioli Nuñez, C. A. (2013). Posibilidade Jurídica da Contestacao da assinatura digital. Revista da SJRJ, 13-38.

Marrero Travieso, Y. (2003). La Criptografía como elemento de la seguridad informática. Acimed, 0-0. Obtenido de eprints.rclis.org

Mendoza Navarro, A. L. (2007). El el Perú los archivos digitales no serán custodiados por los archiveros. Ciencias de la Información, 28-36.

Ministerio de Economía, Fomento y Turismo. Gobierno de Chile. (8 de Febrero de 2013). Ministerio de Economía, Fomento y Turismo. Obtenido de http://www.entidadacreditadora.gob.cl/

3C Tecnología ***(Edición 23)*** *Vol.6 – Nº 3*
Septiembre – diciembre'17, 14 – 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

Ministerio de Industria y Comercio. Subsecretaría de Estado de Comercio de la República de Paraguay. (s.f.). Ministerio de Industria y Comercio. Obtenido de http://www.mic.gov.py/v1/sites/172.30.9.105/files/VERSION%20DEFINITIVA%20AJUSTADA.pdf

Ministerio de Justicia del Perú. (s.f.). Ministerio de Justicia. Obtenido de www.minjus.gob.pe/wp-content/uploads/2014/.../DS-052-2008-pcm.pd

Ministerio Secretaría General de la Presidencia. Proyecto Reforma y Modernización del Estado. (04 de Diciembre de 2013). Sistema Nacional de Información Ambiental SINIA - Chile. Obtenido de www.sinia.cl

Naciones Unidas. (2002). Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001. Obtenido de Uncitral: www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pd

National Institute of Standards and Technology. (25 de Mayo de 2001). NIST. Obtenido de http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

National Institute of Standards and Technology. (Julio de 2013). *National Institute of Standards and Technology.* Recuperado el 2 de Septiembre de 2017, de http://nvlpubs.nist.gov

Network Working Group. (Mayo de 2008). The Internet Engineering Task Force. Obtenido de http://tools.ietf.org/html/rfc5280#section-3.2

Organismo Nacional de Acreditación de Colombia. (04 de Noviembre de 2014). ONAC. Obtenido de http://www.onac.org.co/anexos/documentos/CAMBIOSACTUALIZA/CEA-4%201-10%202015-08-13.pdf

Ortiz Figueroa, G. A. (10 de Junio de 2010). upcommons. Obtenido de http://upcommons.upc.edu/handle/2099.1/9750

Paar, C., & Pelzl, J. (2010). Understanding Cryptography. New York: Springer.

Pario Communications Limited. (10 de Octubre de 2013). vlex. Obtenido de http://international.vlex.com/vid/table-electronic-signature-legislation-469369230

Quintanilla, J., Doren, C., & Hernández, D. (2014). The Electronic Signature in Chile. Digital Evidence and Electronic Signature Law Review, 69-79.

Rani, S., & Kaur, H. (2017). Technical Review on Symmetric and Asymmetric Cryptography Algorithms. *International Journal of Advanced Research in Computer Science*, 182 - 186.

Red Iberoamericana de Protección de datos. (13 de Noviembre de 2013). redip. Obtenido de http://www.redipd.es/legislacion/common/legislacion/Bolivia/DS_1793_Telecomunicaciones.pdf

Registro Nacional de identifiación y estado civil. (11 de Enero de 2013). RENIEC. Obtenido de www.reniec.gob.pe

Reyes, A. A. (2003). *Biblioteca virtual Miguel de Cervantes.* Recuperado el 21 de Agosto de 2017, de www.cervantesvirtual.com

Rivolta, M. (2010). Desarrollo de la Infraestructura de firma digital: resultado de encuesta a expertos. XV Congreso Internacional de CLAD sobre la reforma del Estado y de la Administración pública, (págs. 1-27). Santo Domingo.

Rodriguez Cabrero, J. (Julio de 2007). Revista Dintel. Obtenido de http://www.revistadintel.es/Revista1/DocsNum12/Tribuna/jrodriguez.pdf

Rojas López, M. D., Suarez Botero, D. M., & Meneses Durango, C. N. (2011). Firma digital: Instrumento de transmisión de información a entidades financieras. Avances en Sistemas e Informática, 7-14.

3C Tecnología ***(Edición 23)*** *Vol.6 – Nº 3*
Septiembre – diciembre'17, 14 – 32
Área de Innovación y Desarrollo, S.L.
ISSN: 2254 – 4143
DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n3e23.14-32

RSA Data Security. (1999). *RSA security.* Recuperado el 20 de Agosto de 2017, de http://storage.jakstik.ac.id/rsasecurity/understanding_pki.pdf

RSA Laboratories. (2015). RSA Laboratories. Obtenido de http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs.htm

Salazar, J. F. (2009). Situación normativa de la Sociedade de la Información en Colombia. Criterio Jur[idico, 89-103.

Satizábal Echavarría, I. C. (Marzo de 2007). Tesis Doctorales en Xarxa. Obtenido de www.tdx.cat

Secretaría permanente del SELA. (Mayo de 2012). Red interamericanade ventanillas únicas de comercio exterior. Obtenido de www.redvuce.org/docs/ESP_Publication_Firma_Digital.pdf

Silva Dugarte, M. F. (2011). Certificación electrónica aplicada en Venezuela y su legislación: garantías y desventajas para negociaciones seguras. Visión Gerencial, 205-220.

Solinas, M., Castello, R. J., Tula, L., Gallo, C., Jorge, J., & Bollo, D. (2013). Implementación de una infraestructura de clave pública con herramientas de software libre. 107 - 117.

SUSCERTE. (13 de Febrero de 2012). SUSCERTE. Obtenido de http://www.suscerte.gob.ve/normativas/

Sumalatha, P., & Sathyanarayana, B. (2015). Enhanced Identity Based Cryptography for Efficient Group Key Management in WSN. *International Journal of Application or Innovation in Engineering & Management*, 116-128.

Velandia Ponce, R. (Junio de 2011). Universidad Central de Venezuela. Obtenido de saber.ucv.ve

Ventura, G. (s.f.). Academia Nacional de Derecho y Ciencias Sociales de Córdoba. Obtenido de http://www.acaderc.org.ar/doctrina/firma-digital-analisis-exegetico-de-la-ley-25506-2001

Wang, Y. (Julio de 2012). UNC Charlotte. Obtenido de webpages.uncc.edu

Whitman, M., & Mattord, H. (2012). *Principles of Information Security.* Boston.

Wollinger, T., Guajardo, J., & Paar, C. (2003). Cryptography in Embedded Systems: An Overview. Proceedings of the Embedded World 2003 Exhibition and Conference, (págs. 735 - 744). Nuremberg.