Aplicabilidad de Algoritmos Criptográficos en firmas electrónicas en Ecuador

Applicability of Cryptographic Algorithms in Electronic Signatures in Ecuador

David Galarza G.[1] Alexis Taco C.[1] Viviana Flores C.[1] José Sancho.[1]

[1] Instituto Tecnológico Superior Quito Metropolitano. Carán N3-195 y Calle B (Nueva Tola 2) Quito, Ecuador., dgalarza@itsqmet.edu.ec, agtaco@itsqmet.edu.ec ,vflores@itsqmet.edu.ec, jsancho@itsqmet.edu.ec

ÉLITE 2019, VOL. (1). NÚM. (2)
ISSN: 2600-5875

Recibido: 12/05/2019
Revisado:15/06/2019
Aceptado: 04/08/2019
Publicado: 05/09/2019

RESUMEN:

En esta era digital; en la cual, desde la información personal hasta claves bancarias, pueden caer en manos de entidades o personas que atenten contra nuestra integridad para su propio beneficio, nace la necesidad de protección desde el sentido informático. En este contexto, la criptografía ofrece la oportunidad de cifrar todo nivel de data, para que esta se vea protegida ante ataques cibernéticos. Las empresas públicas de toda Latinoamérica, específicamente entidades bancarias, han optado por varios métodos de cifrado criptográfico, brindando a sus usuarios la facilidad de contar con una firma electrónica. El presente artículo introduce al lector en la teoría de los algoritmos criptográficos; además, presenta un análisis de cómo dichos algoritmos son utilizados en el desarrollo de firmas electrónicas. Se busca de esta manera, determinar cuál es el método de cifrado que mejor se acopla a las necesidades de las empresas ecuatorianas, exponiendo ventajas y desventajas de cada uno los algoritmos matemáticos expuestos.

Palabras clave: criptografía, firmas electrónicas, AES, DES, RSA, CIA, algoritmos.

ÉLITE 2019 VOL 1. NUM 2. ISSN: 2600-5875

ABSTRACT:

In this digital age, which personnel information to bank codes, can fall into the hands of entities or people that may threat our integrity for their own benefit, the need arises to protect such information. In this context, cryptography offers the opportunity to encrypt such information, so that it can be protected against cyber-attacks. Public companies throughout Latin America, specifically banks, have opted for various cryptographic encryption methods, giving their users the facility to retail an electronic signature. This article introduces the reader to the theory of cryptographic algorithms, an analysis of how these algorithms are used in electronic signatures, to tabulate and evidence the standards and algorithms that are mostly used. With this previous analysis, we can define the applicability of these cryptographic standards in electronic signatures of Ecuador. With this, it is possible to determine the best encryption method that matches the needs of Ecuadorian companies, exposing advantages and disadvantages of each mathematical algorithm showed in this document, in order to enrich the utility of electronic signatures or digital certificates, imposing the incorporation of cryptographic algorithms.

Keywords: Cryptography, electronic signatures, AES, DES, RSA, CIA, algorithms.

INTRODUCCIÓN:

La seguridad en los sistemas de información representa no solo un reto, o un desafío, sino un componente fundamental a ser incluido en los requerimientos, y especificaciones de requisitos, como un factor indispensable a considerarse siempre para el análisis, diseño, construcción e implementación en modelos de solución de seguridad informática.

El objetivo principal es garantizar los tres pilares fundamentales de la seguridad informática, los cuales son: confidencialidad, integridad y disponibilidad (CIA) con el objetivo de asegurar el proceso de firmar documentos electrónicos. Dicha información digital firmada tiene la misma validez que un ¡a firma en papel duro o físico, por lo que es indispensable aplicar criterios de seguridad informática en las firmas electrónicas, empezando por el algoritmo de encriptación que estas utilizan. Los criterios jurídicos aplicados a las rubricas digitales, dependen de la política gubernamental de cada país.

A continuación, se realiza un estudio referente a la aplicabilidad de algoritmos criptográficos en firmas electrónicas en Ecuador.

ESTADO DEL ARTE:

En el Ecuador, la firma electrónica tiene inicio en el año 2002 mediante la socialización de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, la cual revela que la rúbrica digital tiene igual validez que una manuscrita. La entidad oficial para la certificación de este procedimiento es el Consejo Nacional de Telecomunicaciones.

La generación del par de claves de la Autoridad de Certificación Raíz y Subordinada, se generan mediante módulos criptográficos Hardware Security Module PKCS#11 (define una interfaz de programación independiente de la tecnología, llamada Cryptoki, para dispositivos criptográficos como tarjetas inteligentes y tarjetas PCMCIA) 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). Steven Marqués revela una vulnerabilidad encontrada y publicada en el código abierto de FIPS propio de OpenSSL (Lie, D. 2018). Por lo que hace que este estándar de cifrado presente un riesgo alto al implementarlo en firmas electrónicas en Ecuador.

Los ataques más comunes relacionados con vulnerabilidades en algoritmos hash, como Cryptoki, utilizados para encriptar firmas electrónicas en Ecuador son:

- Ataque de cumpleaños
- Ataque de mensaje sin sentido
- Ataque de mensaje con sentido

De acuerdo a lo descrito, la firma electrónica reemplaza a la firma manuscrita, por lo que, la pérdida o robo de una de estas, deriva en problemas judiciales y financieros de bajo, mediano o alto riesgo.

MARCO CONCEPTUAL:

Criptografía.

Es la técnica utilizada para cifrar información, utilizando claves o procedimientos basados en algoritmos matemáticos, con la finalidad de que este mensaje cifrado únicamente sea descifrado y entendido por quienes tienen la llave, a pesar de que sea una entidad pública. (Taranilla de la Varga, C. 2018).

Estándares Criptográficos.

Fips 140-2

Es un estándar de seguridad informática para garantizar y acreditar módulos criptográficos, creado por el gobierno de los estados unidos específicamente por la NIST. Posteriormente, se incorporó al estándar en el reconocido OpenSSL para acceso y manipulación de ordenadores a través de consolas y terminales. (Schnieder, E., & Tarnai, G. 2011).

El estándar ofrece, entre otras características, criterios o niveles de seguridad qué garantizan el cumplimiento o balanceo del CIA. La implementación de estos niveles depende directamente del rendimiento estimado desde la perspectiva del qué lo utiliza. Acontinuación se muestran los detalles por nivel en la tabla 1 (FIPS Validation - MOVEit & WS FTP Server, 2018).

Tabla 1: Niveles del estándar FIPS 140-2.

(Elaboración propia)

Nivel	Detalle
Nivel 1	Este módulo criptográfico puede ser ejecutado en sistemas operativos no autorizados
Nivel 2	Incorpora autenticación basada en roles, logs de manipulación y auto recuperación de sistemas operativos.
Nivel 3	Incorpora evidencia de manipulación generalizada y realizada de forma física.
Nivel 4	Agrega resistencia a manipulación, impacto, probabilidad de ocurrencia y riesgos.

Common criteria

Intenta alinear los criterios acerca de seguridad de productos de software utilizados en todo el mundo con la finalidad de estandarizar la evaluación de seguridad en múltiples países. (Herrmann, D. 2013).

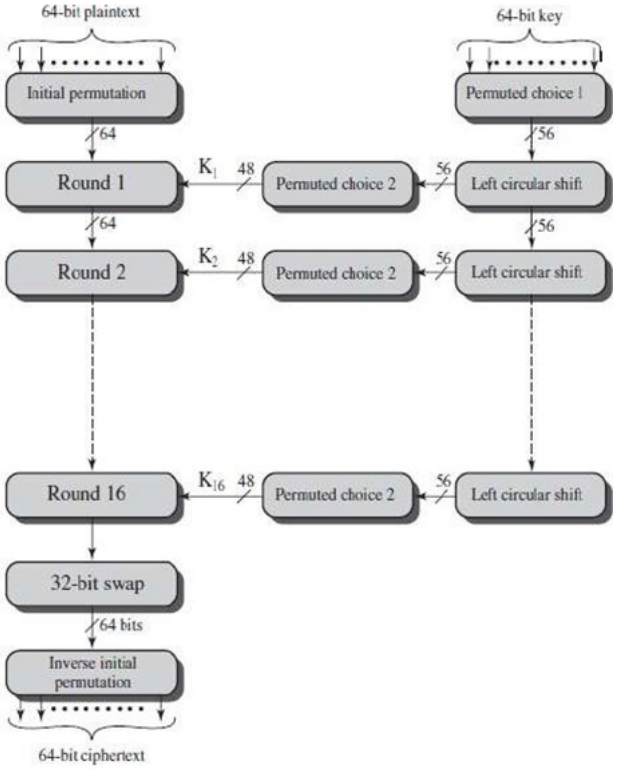
Algoritmos criptográficos

Des

Metodología para cifrar información basado en el estándar FIPS en los estados unidos. Fue diseñado y desarrollado en 1977. (Hankerson, D., Vanstone, S., & Menezes, A. 2009).

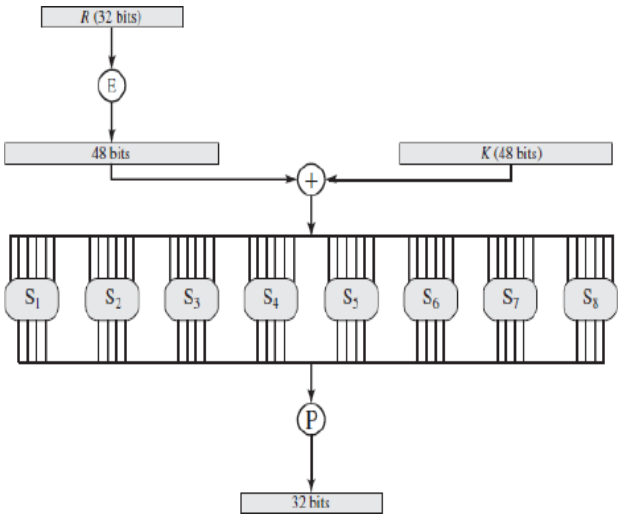
La figura 1 muestra la forma algorítmica en la cual se fundamenta DES para encriptar la información que sirve de insumo en el proceso criptográfico. (Blakely & Chaum, 2013).

Figura 1: Algoritmo general DES. (Stallings, 2012)



A continuación, se presenta en la figura dos el algoritmo matemático qué utiliza DES para encriptar información. Los insumos necesarios son: la clave y los datos de entrada. (Blakely & Chaum, 2013)

Figura 2: Función matemática para encriptación DES. (Stallings, 2012)



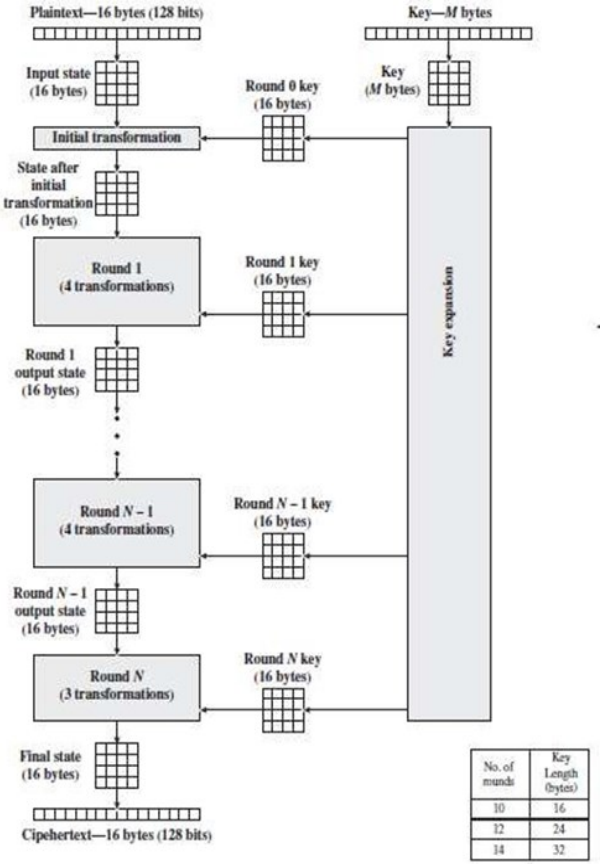
AES

También es conocido como Rijndael, es un algoritmo de cifrado por bloques. Es actualmente el algoritmo más utilizado debido a su capacidad de blindar bajo bloques temáticos a la información. (Hankerson, D., Vanstone, S., & Menezes, A. 2009).

Para el proceso de encriptación de AES es necesario el texto plano y la llave como se puede visualizar en la figura 3. (Daemen & Rijmen, 2011).

Esta llave debe ser distribuida considerando que el portador tendrá la capacidad legal de acceder a la información qué ha sido cifrada, por tanto, para la socialización de la llave se deben considerar incorporar algoritmos qué garanticen la confidencialidad e la misma.

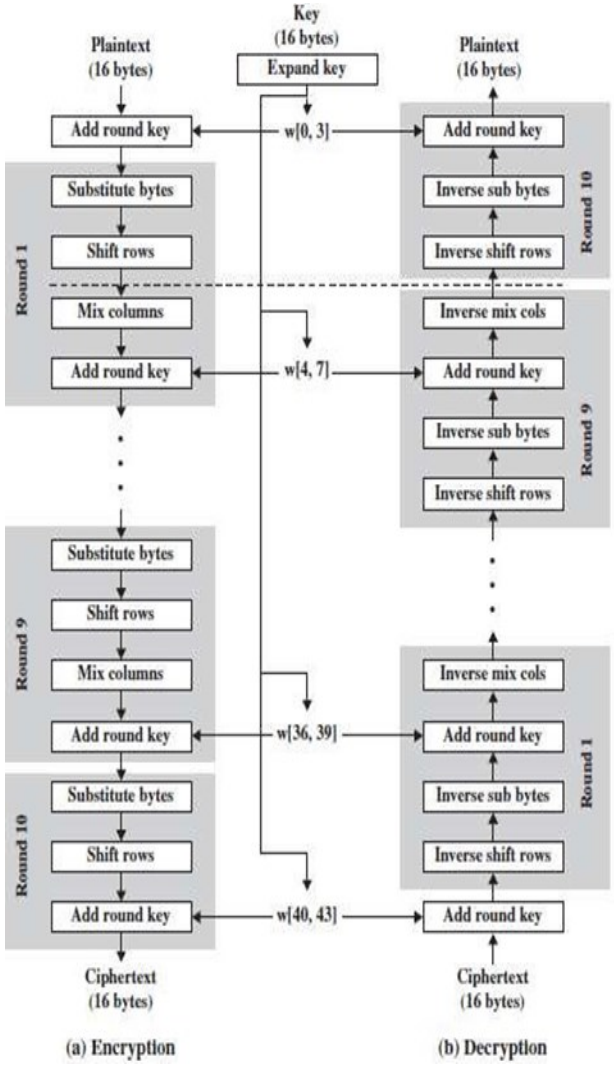
Figura 3: Proceso de encriptación AES. (Stallings, 2012)



La figura 4, presenta el proceso algorítmico inherente a AES, imperioso para realizar encriptacion y desencriptacion de datos. (Daemen & Rijmen, 2011).

La llave generada es utilizada tanto para encriptar como para desencriptar el texto plano, por lo que es sumamente necesario incorporar criterios de seguridad tanto para la creacion, distribucion y utilizacion de esta llave, con la finalidad de garantizar el cumplimiento con los principios del CIA: confidencialidad, integridad y disponibilidad por parte del proceso (Daemen & Rijmen, 2011).

Figura 4: Encriptacion y desencriptacion AES. (Stallings, 2012)



RSA

Es un sistema de criptografía diseñado y desarrollado en 1979. Fue el primer algoritmo en ser utilizado para la encriptación de información. AES es su sucesor por excelencia, ya que brinda rendimiento exponencial respecto a RSA. (Hankerson, D., Vanstone, S., & Menezes, A. 2009).

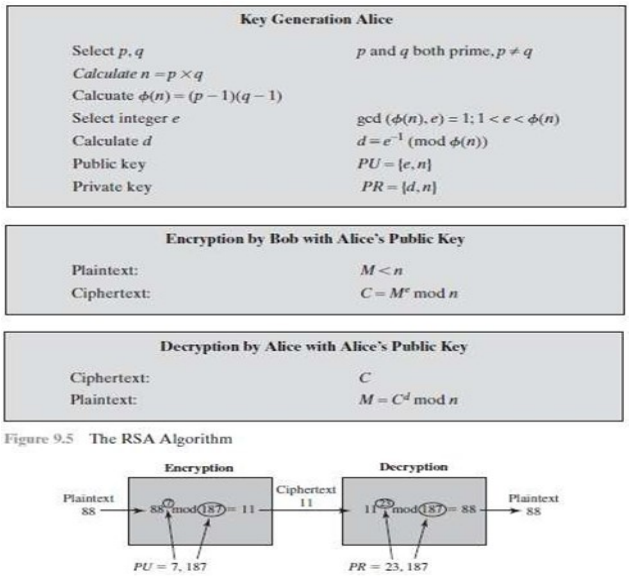
El algoritmo RSA es un bloque cifrado que traduce texto plano a texto cifrado para lo cual hace uso de un rango de enteros entre 0 y n-1, algoritmo implementado para cualquier n. (Stallings, 2012).

Los tamaños típicos de n se encuentran entre 1024 bits o 309 dígitos decimales. Por tanto, n es menor que 2^1024. (Stallings, 2012).

El criterio matemático inherente de RSA hace qué el algoritmo garantice la seguridad en su totalidad, lo que genera bajo rendimiento en términos de agilidad tecnológica. (Abraham, 2012).

A continuación, se presenta el algoritmo RSA en la figura 5:

Figura 5: Algoritmo RSA. (Stallings, 2012)



HASH

Hace referencia a un algoritmo matemático que transforma y traduce cualquier bloque aleatorio de datos en una porción cifrada de un tamaño específico, siempre de 160 bits. Es la huella digital de cualquier documento o información digital sin importar su tamaño. (Hankerson, D., Vanstone, S., & Menezes, A. 2009).

SHA1 - SHA2

Secure Hash Algorithm, es el sucesor de hash, cumpliendo el mismo objetivo. Sin embargo, el nivel de seguridad es mucho más grande que su antecesor. (Hankerson, D., Vanstone, S., & Menezes, A. 2009).

PKCS

Es un grupo de estándares de criptografía que desarrollan e incorporan claves públicas, con la finalidad de socializarlas con la característica de que solo pueden ser utilizados en metadatos fabricados a partir de su llave privada. (Hankerson, D., Vanstone, S., & Menezes, A. 2009).

Firmas digitales

Se entiende por firma digital a un esquema matemático que tiene por objetivo demostrar la autenticidad de un mensaje digital o un documento electrónico. (Hermes, I. 2016).

Firmas electrónicas

Una firma electrónica certifica la vinculación de la rúbrica electrónica con una persona determinada. Equivale directamente a una firma manuscrita, ya que tiene la misma validez legal, jurídica y procedimental según la Ley de Comercio Electrónico. (Registro Civil. 2019).

Aplicación de criptografía en firmas electrónicas en América Latina

Cifrado simétrico.

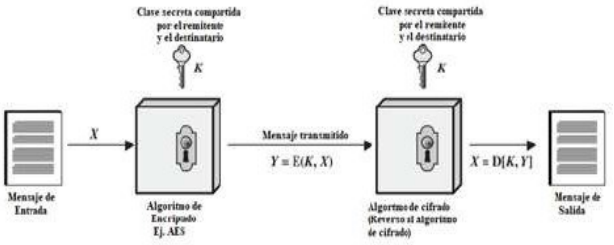
Una de las primeras y más utilizadas formas de cifrado es la criptografía simétrica, también conocida como cifrado convencional o de clave pública. Uno de los más utilizados métodos de cifrado simétrico es el AES, método que se explicará a continuación.

Según (Stallings, 2012) un modelo de cifrado simétrico contiene los siguientes 5 ingredientes:

- Mensaje de entrada: Texto sin formato que se ingresa en el algoritmo de encriptación.
- Algoritmo de encriptado: Serie de pasos lógicos que realizan el cifrado del mensaje de entrada.
- Clave secreta K: es un valor independiente al mensaje de entrada y al algoritmo. El algoritmo producirá una salida distinta dependiendo de la clave específica que se utiliza en ese momento.
- Mensaje transmitido: Es el mensaje codificado que depende del mensaje de entrada y de la clave secreta "K",

La figura 6 muestra el proceso de encriptación simétrico, el cual está compuesto por una clave secreta compartida entre el remitente y el destinatario, y un algoritmo de encriptado para cifrar y descifrar el mensaje. En este caso, la clave de cifrado y de encriptación es la misma, característica propia del cifrado simétrico.

Figura 6: Modelo simplificado de cifrado simétrico. (Stallings, 2012)



Este criterio criptográfico es aplicado en firmas electrónicas basándose en los algoritmos RSA, DSA y ECDSA, los cuales presentan en su arquitectura un complejo problema matemático relacionado con números primos y curvas elípticas con la finalidad de garantizar el nivel de seguridad qué se incorpora en las firmas electrónicas. (Stallings, 2012).

Por tanto, se presenta a continuación los algoritmos criptográficos utilizados en la región de américa latina:

En la Argentina, la firma electrónica se apoya en estándares tecnológicos definidos administrados por la oficina de Tecnologías de Información y sus componentes son (Rivolta, 2010):

- Protocolos qué brindan facilidades de acceso a las llaves públicas por parte de los usuarios.
- Estándares de encriptación y para algoritmos hash.
- Estándares para la creación segura de llaves compartidas.

El estándar utilizado es el **X.509 versión 3**, mientras que el estándar criptográfico utilizado en firmas electrónicas de la República de la Argentina es **FIPS 140-2 nivel 3.**

En Brasil, la firma electrónica se base en una infraestructura de clave pública emitida y administrada por el Instituto de tecnologías de Brasil (ITI). Con la finalidad de cumplir los lineamientos normados por el ITI, la firma electrónica adopta los siguientes estándares (Magioli Nuñez, 2013):

- **FIPS 140-1** o su equivalente.
- **FIPS 140-1 nivel 2**, orientado a cadenas de certificados V0.
- **FIPS 140-2 nivel 2** para cadenas de acreditación V1.
- **FIPS 140-2 nivel 3** para cadenas de certificados V2 y V3 utilizando el algoritmo **ECDSA o RSA.**

En Bolivia, la firma electrónica se encuentra reglamentada por la ley de Telecomunicaciones, Tecnologías de Información y comunicación del país, en la cual establece, al igual que en el resto de países, la normativa que deberán cumplir las entidades emisoras del certificado digital.

Los estándares aplicados son los siguientes (González Cruz, 2005):

- **RFC5280,** en el cual se definen los formatos **X.509 versión 2 y 3.**
- **FIPS 140-2** para la gestión de seguridad de la firma electrónica.

En Chile, las firmas electrónicas están normadas y reguladas desde el 2002 y se dividen en simple y avanzada.

La firma electrónica avanzada en la que permite firmar documentos garantizando su validez legal certificado por un PKI.

Esta es la principal diferencia con la firma simple. Por tanto, la avanzada cumple con estrictos criterios de seguridad por lo que incorpora los siguientes estándares (Ministerio Secretaría General de la Presidencia. Proyecto Reforma y Modernización del Estado, 2013):

- **FIPS 140-2 nivel 2** para administrar llaves criptográficas.
- **Common criteria EAL 3.**

En Colombia, la firma electrónica está basada en la Ley modelo de la Comisión de la Naciones Unidas para el Derecho Mercantil Internacional CNUDMI y adaptada a la ley colombiana la cual supervisa qué la llave pública y certificados digitales deben cumplir con los siguientes criterios (Rojas López, Suarez Botero, & Meneses Durango, 2011):

- Certificado **FIPS 140-2 nivel 3 o superior**
- Clave **RSA 2048 o superior.**

En Paraguay, las firmas electrónicas están supervisadas por el Ministerio de Industria y Comercio, Subsecretaria de Estado de Comercio de la República de Paraguay por lo que, el certificado digital, debe cumplir con (Secretaría permanente del SELA, 2012):

- **Estándar FIPS 140-2 nivel 3** para módulos criptográficos.
- **Estándar FIPS 140-2 nivel 2** para certificados firmados digitalmente por personas.

En Perú, el Instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual es la entidad encargada de la regulación de la firma electrónica en el país, la cual

establece que se debe cumplir como mínimo (Registro Nacional de identificación y estado civil, 2013):

- **El estándar FIPS 140-1 nivel 3** o **Common Criteria EAL4** para la transacción de certificados.
- Para la gestión de certificados se utiliza **FIPS 140-2 nivel 3 y Common Criteria EAL4+.**

En Uruguay, la unidad certificadora es la Agencia para el desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC) qué se alinea directamente con los objetivos de la Presidencia de la República. Las firmas electrónicas deben cumplir con los siguientes criterios para garantizar la seguridad en la transacción de información (Correo Uruguayo, 2011):

- **ITSEC**
- **FIPS 140-1 nivel 3**
- **Common Criteria**

Finalmente, en Venezuela, la entidad reguladora de emisores de certificados digitales es la Superintendencia de Servicios de Certificados Electrónicos que garantiza el cumplimiento con la normativa vigente en el país con respecto a la firma electrónica la cual aplica los estándares (Arcila, C., & De la Barra, R., 2009):

- **ETSI TS 102 042**
- **FIPS 140-2**

A continuación, la tabla 2 presenta un resumen de los estándares criptográficos utilizados en los países de Latinoamérica.

Tabla 2: Estándares y algoritmos por país de América Latina exceptuando a Ecuador. (Elaboración propia).

País	Estándar/Algoritmo
Argentina	**X.509 versión 3, FIPS 140-2 nivel 3**
Brasil	**FIPS 140-1, FIPS 140-1 nivel 2, FIPS 140-2 nivel 2, FIPS 140-2 nivel 3, con algoritmos de ECDSA o RSA inherentes.**
Bolivia	**X.509 versión 2 y 3, RFC5280, FIPS 140-2**
Chile	**FIPS 140-2 nivel 2, Common criteria EAL 3**
Colombia	**FIPS 140-2 nivel 3 o superior, Algoritmo RSA 2048 o superior**
Paraguay	**FIPS 140-2 nivel 3, FIPS 140-2 nivel 2**
Perú	**FIPS 140-1 nivel 3, Common Criteria EAL4, FIPS 140-2 nivel 3, Common Criteria EAL4+**
Uruguay	**ITSEC, FIPS 140-1 nivel 3, Common Criteria**
Venezuela	**ETSI TS 102 042, FIPS 140-2**

El estándar y el algoritmo más comúnmente utilizado para firmas electrónicas en los países de la región es.

- Estándar FIPS 140-2.
- Algoritmo RSA.

Aplicación de estándares criptográficos en firmas electrónicas en Ecuador

En la actualidad, el ente regulador de la emisión de certificados digitales es el Banco Central, el cual tuvo inicio en el año 2002 de acuerdo con la ley de Comercio Electronico, Firmas Electronicas y Mensajeria de Datos. (Banco Central del Ecuador, 2013)

Los módulos criptográficos, estándares y algoritmos qué actualmente se utilizan en Ecuador para la firma electrónica, son (Banco Central del Ecuador, 2013):

- **Módulo de Seguridad de Hardware PKCS#11**
- **FIPS 140-2 nivel 3 o superior**
- **Common Criteria**
- **FIPS 140-2 nivel 2 .**
- **FIPS 1 nivel 2**

Debido a que la firma electrónica ecuatoriana está basada en el estándar FIPS 140-2 y este, a su vez, en el algoritmo criptográfico RSA se presenta la siguiente tabla (tabla 3) ventajas y desventajas que se obtiene de aplicar AES, teniendo en cuenta que este algoritmo es matemáticamente más ligero, lo que proporciona un alto criterio en rendimiento.

Tabla 3: Ventajas y desventajas del algoritmo AES. (Elaboración propia)

Ventajas	Desventajas
Algoritmo matemático ligero lo cual se traduce en alto rendimiento.	La seguridad es dependiente de la clave compartida entre el emisor y el receptor
Encriptacion y desencriptacion utilizando el mismo criterio, lo que se traduce en alto rendimiento	La distribución de las claves se la debe realizar con un criterio de seguridad alto.
Algoritmo abierto y difundido.	Probabilidad alta de ataques debido a qué es un algoritmo ampliamente difundido.

RSA es un algoritmo bastante robusto, sin embargo, de bajo rendimiento en cuestión a tiempos de respuesta por la misma lógica programática qué le da razón a su característica principal de solidez algorítmica. (Stallings, 2012)

DISCUSIÓN DE RESULTADOS:

Como consecuencia de la investigación y experimentación, se obtuvieron los siguientes resultados:

- Los países en Latinoamérica, incluido Ecuador, a nivel de estándar, utilizan para firmas electrónicas con mayor frecuencia: FIPS 140-2, mientras qué a nivel algorítmico incorporan: RSA
- Los criterios de estándares y algoritmos criptográficos fueron pre establecidos y normados bajo la legislación de cada país.

- El algoritmo RSA es el que con mayor frecuencia es usado para firmas electrónicas debido a su alto criterio de seguridad, sin embargo, el rendimiento no es el esperado.

CONCLUSIONES

De acuerdo con el estudio realizado en el presente documento se han considerado importante incluir las siguientes recomendaciones:

- Para firmas electrónicas a nivel regional se utiliza el algoritmo criptográfico RSA debido a que garantiza la seguridad, a pesar de ello, se considera un criterio algorítmico de baja productividad.
- Si se incorpora AES en algoritmos criptográficos se debe considerar que el nivel de seguridad no es el esperado.
- No se puede cambiar el criterio de aseguramiento de firmas electrónicas en Ecuador sin antes modificar la ley y los procesos legales qué gestionan los certificados digitales.
- La aplicabilidad del algoritmo AES es viable en firmas electrónicas ecuatorianas, no obstante, se debería replantear el criterio jurídico y procedimental para llevar a cabo esta implementación considerando que el criterio algoritmo de AES es vulnerable.

RECOMENDACIONES

Considerando el estudio y la investigación con respecto a la aplicabilidad de algoritmos criptográficos en firmas electrónicas del Ecuador, se ha estimado imperioso redactar las siguientes:

- Si se procediera con la incorporación del algoritmo AES, se recomienda utilizar criterios de RSA para garantizar la seguridad.
- Si se mantiene el algoritmo RAS como principal método criptográfico en firmas electrónicas, es recomendable incorporar la ligereza de AES para agilizar las transacciones de documentación genérica.
- Se recomienda mantener RSA en documentación o información sensible y crítica.

REFERENCIAS BIBLIOGRAFÍCAS:

1. Abraham, A. (2012). Proceedings of the 2012 World Congress on Information and Communication Technologies. Piscataway, NJ: IEEE.

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

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

4. Blakely, G., & Chaum, D. (2013). Advances in Cryptology (6th ed.). New York: Springer.

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

6. Daemen, J., & Rijmen, V. (2011). The design of Rijndael (5th ed.). Berlin: Springer.

7. FIPS Validation - MOVEit & WS FTP Server. (2018). Retrieved 5 February 2020, from https://www.ipswitch.com/industries/gover nment/government-us-federal- government/fips-validation/

8. Firma Electrónica – Registro Civil. (2019). Retrieved 12 December 2019, from https://www.registrocivil.gob.ec/certificado-de-firma-electronica/

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

10. Hankerson, D., Vanstone, S., & Menezes, A. (2009). Guide to Elliptic Curve Cryptography. New York: Springer-Verlag.

11. Hermes, I. (2016). ¿Qué es la firma digital? Retrieved 12 December 2019, from http://www.firma-digital.cr/que_es/

12. Herrmann, D. (2013). Using the common criteria for IT security evaluation. Boca Raton: Auerbach Publications.

13. Lie, D. (2018). Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security.

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

15. 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

16. Registro Nacional de identificación y estado civil. (11 de enero de 2013). RENIEC. Obtenido de www.reniec.gob.pe

17. 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 Administra-pública, (págs. 1-27). Santo Domingo.

18. 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

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

20. Schnieder, E., & Tarnai, G. (2011). Formal methods for automation and safety in railway and automotive systems. Heidelberg: Springer.

21.Stallings, W. (2012). Cryptography and Network Security (5th ed.). New Jersey: Pearson.

22. Taranilla de la Varga, C. (2018). Criptografía (1st ed.). Córdoba: Guadalmazán.