ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

DIRECCIÓN DE POSGRADO

MAESTRIA EN GERENCIA DE REDES Y TELECOMUNICACIONES
I PROMOCIÓN

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER

TEMA: ANÁLISIS TÉCNICO PARA BRINDAR EL SERVICIO DE FIRMA ELECTRÓNICA POR LA DIRECCIÓN GENERAL DE REGISTRO CIVIL, IDENTIFICACIÓN Y CEDULACIÓN

AUTOR: ING. PACHACAMA CUEVA, PILAR

DIRECTOR: ING. SILVA, RODRIGO MSc.

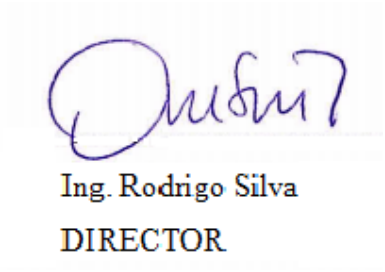
SANGOLQUI
2015

CERTIFICADO DIRECTOR Y OPONENTE

CERTIFICACIÓN

Certificamos que el presente trabajo titulado "ANALISIS TÉCNICO PARA BRINDAR EL SERVICIO DE FIRMA ELECTRONICA POR LA DIRECCIÓN GENERAL DE REGISTRO CIVIL, IDENTIFICACIÓN Y CEDULACIÓN" realizado por la Ing. Pilar Pachacama ha sido dirigido y revisado a través de reuniones periódicas, y cumple las normas estatutarias establecidas en el Reglamento de Estudiantes de la Universidad de las Fuerzas Armadas.

Sangolquí, Mayo de 2015



Ing. Rodrigo Silva
DIRECTOR

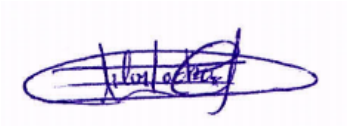
Crnl. Edwin Chávez
OPONENTE

AUTORÍA DE RESPONSABILIDAD

La abajo firmante, en calidad de egresada de la Maestría Gerencia de Redes de Telecomunicaciones; declaro que los contenidos del proyecto de grado denominado "ANALISIS TÉCNICO PARA BRINDAR EL SERVICIO DE FIRMA ELECTRONICA POR LA DIRECCIÓN GENERAL DE REGISTRO CIVIL, IDENTIFICACIÓN Y CEDULACIÓN", requisito previo a la obtención del Grado de Magíster en Gerencia de Redes y Telecomunicaciones, son absolutamente originales, auténticos, personales, han sido desarrollados con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que se incluyen en este documento, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi auditoria.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance Científico del proyecto de grado en mención.

Sangolquí, Mayo de 2015

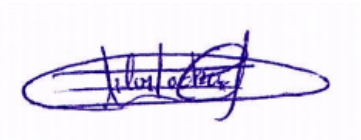


Ing. Pilar Pachacama
Autor

AUTORIZACIÓN

Yo, Ing. Pilar Pachacama, autorizo a la Universidad de las Fuerzas Armadas la publicación en la biblioteca virtual de la Institución el proyecto de tesis titulado "ANALISIS TÉCNICO PARA BRINDAR EL SERVICIO DE FIRMA ELECTRONICA POR LA DIRECCIÓN GENERAL DE REGISTRO CIVIL, IDENTIFICACIÓN Y CEDULACIÓN", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y auditoría.

Sangolquí, Mayo de 2015



Ing. Pilar Pachacama
Autor

DEDICATORIA

A mis padres José Luis y María Guadalupe que con su ejemplo de trabajo, honestidad y su amor supieron guiarme durante mi vida para conseguir mis objetivos.

Pilar Pachacama Cueva

AGRADECIMIENTO

Agradezco de manera especial a mi Director, Ing. Rodrigo Silva por su acertada guía para el desarrollo de este trabajo, a la Dirección General de Registro Civil, Identificación y Cedulación, a la Subsecretaria de Asuntos Postales y Registro Civil del Ministerio de Telecomunicaciones y de la Sociedad de la Información y a todas las personas que contribuyeron directa o indirectamente con la elaboración de este proyecto.

ÍNDICE DE CONTENIDO

CERTIFICADO DIRECTOR Y OPONENTE ii
AUTORÍA DE RESPONSABILIDAD iii
AUTORIZACIÓN iv
DEDICATORIA v
AGRADECIMIENTO vi
ÍNDICE DE CONTENIDO vii
RESUMEN xiii
ABSTRACT xiv
CAPÍTULO I 1
PLAN DE PROYECTO Y JUSTIFICACIÓN 1
1.1 INTRODUCCIÓN 1
1.2 PROYECTO Y JUSTIFICACIÓN 1
1.2.1 Tema del Proyecto 1
1.2.2 Planteamiento, Formulación y Sistematización del Problema 1
1.2.3 Objetivos de la Investigación 3
1.2.4 Justificación del Estudio 4
1.2.5 Alcance de la Investigación 5
1.2.6 Estado del arte a nivel mundial de la firma electrónica 5
1.2.7 Firma Digital y firma electrónica en el Ecuador 9
1.2.8 La Dirección General de Registro Civil, Identificación y Cedulación 10
1.2.9 Infraestructura de la DIGERCIC - Análisis de la Situación Actual 10
CAPÍTULO II 21
MARCO TEORICO Y CONCEPTUAL 21
2.1 MARCO TEÓRICO 21
2.1.1 Criptografía 21
2.1.2 Criptografía simétrica 21
2.1.3 Criptografía asimétrica 22
2.1.4 Sistemas de información y su clasificación 22
2.2 MARCO CONCEPTUAL 23
2.2.1 Comercio Electrónico 24
2.2.2 Firma digital. 24

2.2.3 Firma electrónica 26
2.2.4 Certificado de firma electrónica 26
2.2.5 Infraestructura de llaves públicas (PKI) 26
2.2.6 Componentes PKI 27
2.2.7 Autoridades Certificadoras (ACs) 29
2.2.8 Autoridad de Registro (AR) 31
2.2.9 Repositorio 31
2.2.10 Emisor CRL 32
2.2.11 Arquitecturas PKI 32
2.2.12 Estructuras de datos PKI 35
CAPÍTULO III 41
METODOLOGIA DE LA INVESTIGACIÓN 41
3.1 METODOLOGÍA DE LA INVESTIGACIÓN 41
3.1.1 Requisitos para Entidades de certificación / Infraestructura de Clave Pública – PKI 42
3.1.2 Requisitos para Hardware Security Module – HSM 44
3.1.3 Requisitos para Tarjetas Inteligentes 44
3.1.4 Método de investigación, técnicas e instrumentos de recolección y procesamiento de datos e información. 46
CAPÍTULO IV 47
EVALUACIÒN DE LOS REQUISITOS TECNICOS 47
4.1 ANÁLISIS DEL CUMPLIMIENTO DE LA NORMA ISO 27001:2005 SISTEMA DE INFORMACIÓN DE GESTIÓN DE LA SEGURIDAD 47
4.1.1 A.5 Políticas de Seguridad 47
4.1.2 A.6 Aspectos Organizativos de la Seguridad de la Información 48
4.1.3 A.7 Gestión de Activos 48
4.1.4 A.8 Seguridad en la Contratación de los Recursos Humanos 49
4.1.5 A.9 Seguridad Física y Ambiental 50
4.1.6 A.10 Gestión de Comunicaciones y Operaciones 50
4.1.7 A.11 Control de Acceso 51
4.1.8 A.12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información 52
4.1.9 A.13 Gestión de Incidentes de Seguridad de la Información 53
4.1.10 A.14 Gestión de la Continuidad del Negocio 54

4.1.11 A 15 Cumplimiento de reglamentación 54
4.2 PRUEBAS DE SEGURIDAD EN LOS SISTEMAS DE LA DIGERCIC..... 55
4.2.1 Pruebas Externas 55
4.2.2 Pruebas Internas 59
4.3 PRUEBAS DE LECTURA Y SEGURIDADES DE LA TARJETA DE IDENTIFICACIÓN 60
4.4 EVALUACIÓN DE REQUISITOS PARA ENTIDADES DE CERTIFICACIÓN / INFRAESTRUCTURA DE CLAVE PÚBLICA – PKI 63
4.4.1 Requisitos para Hardware Security Module – HSM 66
4.4.2 Requisitos para Tarjetas Inteligentes 66
4.5 EVALUACIÓN DE LAS SEGURIDADES DE LA INFORMACIÓN DE LAS TARJETAS DE IDENTIFICACIÓN 68
4.5.1 Seguridades de la tarjeta de identificación 68
4.5.2 Normas y requisitos físicos de la tarjeta de identidad 69
4.5.3 Especificaciones del chip: 69
4.5.4 Características electromagnéticas, químicas, físicas y mecánicas 71
4.6 ESTADÍSTICAS DE PÉRDIDA DE DOCUMENTOS PERSONALES Y FALSIFICACIÓN DE FIRMA O DOCUMENTOS 75
4.6.1 Distrito Metropolitano de Quito 75
4.6.2 Guayaquil 76
4.7 ESTADÍSTICAS DE USO (REAL) DEL DNI ELECTRÓNICO EN ESPAÑA .. 77
4.7.1 Ciudadanos con DNIe 77
4.7.2 Validaciones de firma e identidad electrónica 77
4.8 DISPOSITIVOS DE ALMACENAMIENTO DE CERTIFICADOS DIGITALES TARJETA CRIPTOGRÁFICA, TOKEN USB 78
4.8.1 Tarjeta Criptográfica de la cédula 78
4.8.2 Token USB 79
4.9 INFRAESTRUCTURA FIRMA ELECTRÓNICA ECUADOR 79
4.10 ANÁLISIS DE FORTALEZAS, OPORTUNIDADES, DEBILIDADES Y AMENAZAS DIGERCIC 83
4.10.1 Evaluación interna 83
4.10.2 Evaluación externa 84
CAPÍTULO V 85
PROPUESTA TÉCNICA 85

5.1 INFRAESTRUCTURA DE FIRMA ELECTRÓNICA PARA LA REPÚBLICA DEL ECUADOR 85
5.1.1 Entidad de Acreditación y Control de Certificación Electrónica (EACCE) .. 86
5.1.2 Autoridad de Certificación Raíz del Ecuador (ACREC) 88
5.1.3 Entidades de Certificación de Información y Servicios Relacionados (EC).. 88
5.1.4 Usuarios 88
5.1.5 Terceros usuarios 88
5.1.6 Diagrama de Flujo del proceso de certificación electrónica 89
5.2 Arquitectura PKI DIGERCIC 89
5.3 AUTORIDAD DE CERTIFICACIÓN PKI PARA EL SERVICIO DE FIRMA ELECTRÓNICA 91
5.3.1 Atributos operativos de la autoridad AC 91
5.3.2 Tipo de Hardware con HSM y aplicación Software 94
5.3.3 Servidor de Autoridad de Certificación Subordinada 96
5.3.4 Servidor de Autoridad de Registro 97
5.3.5 Servidor de Autoridad de Validación 98
5.3.6 Infraestructura de Clave Pública Firma Electrónica DIGECIC 100
5.3.7 Servidor Autoridad de Sellado de Tiempo 100
5.3.8 Servidor de Firma Electrónica 102
5.4 TIPOS DE DISPOSITIVOS, SISTEMAS OPERATIVOS Y ESTÁNDARES PARA ACCESO AL CHIP DE LA TARJETA ELECTRÓNICA 104
5.5 ORGANIGRAMA ESTRUCTURAL DE LA UNIDAD DE NEGOCIOS DE CERTIFICACIÓN DIGITAL – UNCD DE LA DIGERCIC 105
5.5.1 Flujograma del proceso de Certificación Digital 106
CAPÍTULO VI 108
CONCLUSIONES Y RECOMENDACIONES 108
BIBLIOGRAFIA 111
ABREVIATURAS Y ACRÓNIMOS 113
ANEXO A 116

INDICES DE TABLAS

Tabla 1. Información Chip Cédula 20
Tabla 2. Entidades de Certificación /Infraestructura de Clave Pública – PKI 42
Tabla 3. Requisitos para Hardware Security Module 44
Tabla 4. Requisitos para Tarjetas Inteligentes 44
Tabla 5. Requisitos Certificación 45
Tabla 6. Otros Requisitos 45
Tabla 7. Lista de puertos abiertos servidor web 57
Tabla 8. Lista de puertos abiertos servidor 60
Tabla 9. Cumplimiento Requisitos para Entidades de certificación / Infraestructura de Clave Pública – PKI 63
Tabla 10. Cumplimiento Requisitos para Hardware Security Module – HSM 66
Tabla 11. Cumplimiento Requisitos para Tarjetas Inteligentes 66
Tabla 12. Cumplimiento Requisitos para Certificación 67
Tabla 13. Cumplimiento Otros Requisitos 67
Tabla 14. Número de certificados emitidos, revocados y vigentes 81
Tabla 15. Número de certificados emitidos, revocados y vigentes por provincia 82
Tabla 16. Número de certificados emitidos, revocados y vigentes por entidad de certificación 82
Tabla 17. Fortalezas y Debilidades - DIGERCIC 83
Tabla 18. Oportunidades y Amenazas - DIGERCIC 84

INDICE DE CUADROS

Cuadro 1. Vulnerabilidades Servidor Web 57
Cuadro 2. Vulnerabilidades Servidor Correo 58
Cuadro 3. Vulnerabilidades Servidor Magna 60
Cuadro 4. Estadísticas de Asalto y robo a personas en Quito 75
Cuadro 5. Estadísticas de Robo a personas en Quito 75
Cuadro 6. Estadísticas de Hurto a personas en Quito 76
Cuadro 7. Estadísticas de certificado de firma electrónica DNIe de España 78

INDICES DE FIGURAS

Figura 1. Esquema Red DIGERCIC 11
Figura 2. Arquitectura Magna 12
Figura 3. Arquitectura Magna- DIGERCIC 14

Figura 4. Evolución DNI 18
Figura 5. Firma Digital 25
Figura 6. : Componentes PKI 29
Figura 7. Arquitecturas PKI- Infraestructura Jerárquica 34
Figura 8. Arquitecturas PKI- Infraestructura en malla 35
Figura 9. Certificado Digital X.509 versión 3 38
Figura 10. Estructura de una CRL 40
Figura 11. Aspectos Organizativos de la seguridad de la información en la DIGERCIC 48
Figura 12. Gestión de Activos 48
Figura 13. Seguridad en la contratación de los recursos humanos de la DIGERCIC 49
Figura 14. Seguridad Física y Ambiental de la DIGERCIC 50
Figura 15. Gestión de Comunicaciones y Operaciones de la DIGERCIC 50
Figura 16. Control de Acceso de la DIGERCIC 51
Figura 17. Adquisición, desarrollo y mantenimiento de los sistemas de información de la DIGERCIC 52
Figura 18. Gestión de incidentes de seguridad de la información de la DIGERCIC 53
Figura 19. Gestión de la continuidad del negocio de la DIGERCIC 54
Figura 20. Cumplimiento de reglamentación en la DIGERCIC 54
Figura 21. Traceroute www.registrocivil.gob.ec 56
Figura 22. Traceroute mailserver.registrocivil.gob.ec 56
Figura 23. Resultado Escaneo puertos TCP 57
Figura 24. Resultado Escaneo puertos UDP 57
Figura 25. Resultado Escaneo puertos UDP 59
Figura 26. Esquema Lectura datos de la cédula 61
Figura 27. Seguridades Anverso Cédula 68
Figura 28. Seguridades Reverso Cédula 69
Figura 29. Estadísticas de Falsificación de firma o documentos y perdida de documentos – Guayaquil 76
Figura 30. Infraestructura Actual de Firma Electrónica Ecuador 81
Figura 31. Modelo Infraestructura Nacional de Certificación Electrónica a nivel jerárquico 86
Figura 32. Diagrama de Flujo del proceso de certificación electrónica 89
Figura 33. Estructura PKI recomendada por la OACI para la emisión de pasaportes electrónicos 90
Figura 34. Modelo PKI DIGERCIC 91
Figura 35. Esquema Autoridad de Certificación DIGERCIC 100
Figura 36. Esquema Autoridad de Sellado de Tiempo - TSA DIGERCIC 102
Figura 37. Acceso Tarjeta Electrónica 104
Figura 38. Organigrama de UNCD - DIGERCIC 106
Figura 39. Flujograma del proceso de Certificación Digital 107

RESUMEN

En el presente trabajo se realiza un completo análisis técnico para determinar si la Dirección General de Registro Civil identificación y Cedulación – DIGERCIC puede implementar el servicio de firma electrónica en el Ecuador. Se realiza un análisis técnico de los requisitos que debe cumplir la DIGERCIC para acreditarse como Entidad de Certificación de Información y Servicios Relacionados, de acuerdo con la Ley de Comercio Electrónico, su Reglamento y de la "Guía de Acreditación de Entidades de Certificación EC Versión 3.3" emitida por el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual. Se verifica nivel de cumplimiento por parte de la DIGERCIC de la Norma ISO 27001:2005 Sistema de Información de Gestión de la Seguridad basada en sus 11 áreas de control. Se realizan pruebas técnicas en los sistemas de la DIGERCIC sobre los cuales se apoyará el servicio de firma electrónica. Además se realiza pruebas de lectura de los datos almacenados en el chip de la cédula y se evalúan las seguridades de la información que se encuentran implementadas en la cédula electrónica. Finalmente se realiza un análisis FODA de la DIGERCIC que permite tomar decisiones sobre la implementación del servicio de firma electrónica. En base a los resultados obtenidos se presenta una propuesta de un modelo jerárquico de Infraestructura de Firma Electrónica para la república del Ecuador y una propuesta para la implementación de una infraestructura de clave pública que permita ofrecer el servicio de firma electrónica por parte de la DIGERCIC.

PALABRAS CLAVES:

- **FIRMA ELECTRÓNICA**
- **ENTIDADES DE CERTIFICACIÓN**
- **INFRAESTRUCTURA DE CLAVE PÚBLICA**
- **DOCUMENTO DE IDENTIDAD NACIONAL**
- **CEDULA ELECTRÓNICA**

ABSTRACT

In this project, a complete technical analysis is performed to determine whether the Directorate General of Civil Registration and Certification Identification - DIGERCIC can implement an electronic signature service in Ecuador. A technical analysis of the requirements to be met by DIGERCIC for its accreditation as Certification Body for Information and Related Services, according to the Electronic Commerce Act, its Regulations and the "Guidelines for the Accreditation of Certification Bodies EC Version 3.3" is issued by the National Institute for the Defense of Competition and Protection of Intellectual Property. The level of compliance is verified by the DIGERCIC of ISO 27001: 2005 and the Information System Security Management based on its 11 control areas. Technical tests in the DIGERCIC systems on which the service will support electronic signature are performed. Besides, reading test data stored in the chip of the identity card and information security that are implemented in the electronic identification are evaluated and performed. Finally, a SWOT analysis of the DIGERCIC that allows decisions on the implementation of electronic signature service is performed. Based on the obtained results, a proposal for a hierarchical model of electronic signature infrastructure for the Republic of Ecuador and a proposal for implementing a public key infrastructure that allows the service to offer electronic signature by the DIGERCIC takes place.

KEYWORDS

- **ELECTRONIC SIGNATURE**
- **CERTIFICATE AUTHORITIES**
- **PUBLIC KEY INFRAESTRUCTURE**
- **DOCUMENT OF NATIONAL IDENTITY**
- **ELECTRONIC IDENTIFICATION**

CAPÍTULO I
PLAN DE PROYECTO Y JUSTIFICACIÓN

1.1 INTRODUCCIÓN

El Ministerio de Telecomunicaciones (MINTEL), organismo rector del desarrollo de las Tecnologías de la Información y Comunicación en el Ecuador, emite políticas, planes, programas y proyectos relativos a las TICs. El MINTEL requiere conocer la factibilidad técnica para la implementación del servicio de firma electrónica por parte de la Dirección General de Registro Civil identificación y Cedulación (DIGERCIC) en el Ecuador.

En el presente trabajo se realizará un análisis técnico de los requisitos que debe cumplir la DIGERCIC para acreditarse como entidad de prestación de servicios de firma electrónica y de certificación de Sello de Tiempo, de acuerdo con la Ley de Comercio Electrónico y su Reglamento. Se realizarán evaluaciones sobre la plataforma utilizada por la DIGERCIC para probar parámetros de Privacidad, Seguridad de la Información, Seguridad Física, Políticas de Certificado de Firma Electrónica y Sello de Tiempo, previos a la implementación de estos servicios en el Registro Civil del Ecuador.

1.2 PROYECTO Y JUSTIFICACIÓN

1.2.1 Tema del Proyecto

Análisis Técnico para brindar el servicio de firma electrónica por la Dirección General de Registro Civil, Identificación y Cedulación.

1.2.2 Planteamiento, Formulación y Sistematización del Problema

1.2.2.1 Planteamiento del problema

El Ministerio de Telecomunicaciones requiere conocer la factibilidad técnica para la implementación del servicio de firma electrónica por parte de la Dirección General de Registro Civil identificación y Cedulación (DIGERCIC) en el Ecuador.

A partir del año 2009 la DIGERCIC emprendió el proyecto de modernización del Sistema Nacional de Registro Civil Identificación y Cedulación enfocado a

definir acciones prioritarias que llevaran a cabo la reestructuración y modernización de la Dirección a nivel nacional, implementando tecnología de punta en lo que respecta a la identificación pública con la finalidad de servir al cliente interno y externo de manera eficiente, ofreciendo calidad y calidez de servicios.

Como parte del proyecto de modernización el Registro Civil adquirió el sistema nacional de identificación electrónica - Sistema Magna que permite la emisión de nuevas tarjetas de identificación electrónicas basado en sistemas biométricos, además de la emisión de certificados de nacimiento, defunción, matrimonio. La tarjeta de identificación electrónica contiene un chip RFID que permite implementar aplicaciones como match on card, epicrisis, firma digital, monedero electrónico. Además de ello la DIGERCIC ha invertido en la modernización de su infraestructura civil y tecnológica a nivel nacional en un valor estimado de $ 70 millones (Dirección General de Registro Civil, Identificación y Cedulación, 2013).

1.2.2.2 Formulación del problema a resolver

La Dirección General de Registro Civil, Identificación y Cedulación dentro de su Plan Estratégico 2012 -2015 incluye la ejecución de un proyecto para implementar el servicio de firma digital y obtener la acreditación por parte del CONATEL / ARCOTEL como Entidad de Certificación de Información y Servicios Relacionados, para ello debe realizar una evaluación de la capacidad tecnológica, capacidad operativa de la DIGERCIC para brindar el servicio de firma electrónica. Dentro de la evaluación de la capacidad tecnológica se debe evaluar al sistema nacional de identificación electrónica - Sistema MAGNA y la tarjeta de identificación electrónica, los mecanismos de seguridad para evitar la falsificación de certificados, precautelar la integridad, resguardo de documentos, protección contra siniestros, control de acceso y confidencialidad durante la generación de claves, también se debe verificar la existencia de sistemas de seguridad, estándares de seguridad, sistema de respaldo de la información que maneja el Registro Civil; además se debe realizar una evaluación de la infraestructura operativa actual del Registro Civil.

El proyecto de firma electrónica tiene el propósito de explotar las funcionalidades de la nueva plataforma tecnológica y de las nuevas tarjetas de

identificación y aprovechar la capacidad instalada de la DIGERCIC a través del proyecto de modernización. En este contexto, las preguntas que se pretende responder en esta investigación son las siguientes:

¿Es suficiente la infraestructura actual de la DIGERCIC para brindar el servicio de firma electrónica?

¿Qué elementos son necesarios considerar para implementar la firma electrónica a través del sistema nacional de identificación electrónica - Sistema MAGNA?

¿Es técnicamente factible la implementación del servicio de firma electrónica por parte del Registro Civil?

1.2.2.3 Hipótesis

La Dirección General de Registro Civil Identificación y Cedulación dispone los elementos y recursos técnicos necesarios para brindar el servicio de firma electrónica en el Ecuador.

1.2.3 Objetivos de la Investigación

1.2.3.1 Objetivo General

Realizar un análisis técnico para verificar si la Dirección General de Registro Civil identificación y Cedulación puede implementar el servicio de firma electrónica en el Ecuador.

1.2.3.2 Objetivos Específicos

- Analizar los sistemas e infraestructura actual de la DIGERCIC
- Realizar pruebas técnicas en los sistemas de la DIGERCIC sobre los cuales se apoyará el servicio de firma electrónica.
- Evaluar las seguridades de la información de las tarjetas de identificación utilizadas para la implementación del servicio de firma electrónica.
- Elaborar una propuesta técnica para la implementación de la firma electrónica para la DIGERCIC.

1.2.4 Justificación del Estudio

La firma electrónica en el Ecuador está regulada desde el año 2002 por la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos (Ley 67) y su Reglamento General de aplicación. En el año 2008 el CONATEL acreditó mediante Resolución 481-20-CONATEL-2008 al Banco Central del Ecuador como la primera Entidad de Certificación de Información y Servicios Relacionados. En el Ecuador existen 4 entidades certificadoras: Banco Central del Ecuador, ANF Autoridad de Certificación, Security Data y el Concejo de la Judicatura.

Las Normas y Reglamentos en el país referentes a Entidades de Certificación de Información y Servicios que se encuentran vigentes son:

- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
- Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
- DECRETO 1356 29-SEP-2008 - Reformas al Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
- DECRETO 867 1-SEP-2011 - Reformas al Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
- RES 370-08-CONATEL-2011 -Pago Terceros Vinculados
- RES 477-20-CONATEL-2008-Modelo de Acreditación
- RES 479-20-CONATEL-2008 - Reglamento Registro Público Entidades
- RES 480-20-CONATEL-2008 - Valores para Acreditación
- Acuerdo Ministerial 181

El Servicio Nacional de Aduanas del Ecuador (Senae) el 8 de febrero de 2013 fusionó el nuevo sistema aduanero Ecuapass con la Ventanilla Única de Comercio Exterior para que por medio de una página web o ventanilla única se pueda realizar todo trámite aduanero de forma inmediata con el uso de certificados de firma electrónica.

En el Ecuador a partir del 01 de enero de 2013 la factura electrónica es opcional y será obligatoria a partir del año 2014. Este nuevo mecanismo de facturación permitirá facturar de manera electrónica, disminuyendo costos y ayudando al medio ambiente. Es una solución que permite la generación, firma y envío de comprobantes de venta, retención o documentos complementarios

tributarios electrónicos, para ello los emisores de la factura deben contar con un certificado de firma electrónica. La factura electrónica es un archivo en XML, que solo puede ser entendido por los sistemas del SRI, los usuarios recibirán un archivo adicional en formato PDF en el que estará el detalle de sus consumos.

1.2.5 Alcance de la Investigación

El presente trabajo abarca el análisis técnico de la nueva infraestructura tecnológica con que cuenta la DIGERCIC: sistema MAGNA y nueva cédula electrónica sobre los cuales se apoyará el servicio de firma electrónica, así como una evaluación de las 11 áreas de control de la norma ISO 27001 para medir el nivel de cumplimiento de la norma ISO 27001:2005 Sistema de Información de Gestión de la Seguridad por parte de la DIGERCIC.

Se han realizado pruebas técnicas de lectura de los datos que se encuentran en el chip de la cédula electrónica y se han evaluado las seguridades de la información de las tarjetas de identificación, así como la verificación de las capacidades de almacenamiento y estándares que cumple para la implementación del servicio de firma electrónica. Además se realiza un análisis de ventajas y desventajas que tiene la cédula electrónica con respecto a otros medios de almacenamiento de certificados digitales.

En base a los resultados del análisis realizado se ha elaborado una propuesta técnica para la implementación de la firma electrónica para la DIGERCIC.

1.2.6 Estado del arte a nivel mundial de la firma electrónica

América Latina y el Caribe

De acuerdo con el documento "Fundamentos de la firma digital y su estado del arte en América Latina y el Caribe", publicado en junio de 2012 por la Secretaría Permanente del Sistema Económico Latinoamericano y del Caribe (SELA), el estado del arte de la firma digital y/o electrónica en la región (Sistema Económico Latinoamericano y del Caribe SELA, 2012) indica que:

Muchos de los países han adoptado la ley modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL por sus siglas en inglés) en su estructura y alcance, adaptándola según sus necesidades, aunque con homogeneidad en los propósitos generales y equivalencias funcionales.

Se destaca que la gran mayoría de los países de la región cuentan con leyes que brindan validez jurídica al comercio electrónico, haciendo que las transacciones en línea sean seguras al permitir la identificación en forma fehaciente de los sujetos que realicen transacciones electrónicas.

Asimismo, refleja cómo "la mayoría de los países latinoamericanos y caribeños han hecho esfuerzos importantes en el diseño e instrumentación de políticas públicas de gobierno electrónico sustentadas en el "cero papel", con miras a promover la transparencia, la seguridad, la eficiencia y la eficacia administrativa" (Sistema Económico Latinoamericano y del Caribe SELA, 2012, pág. 6).

Los trámites por medios electrónicos más comunes tienen que ver con los servicios que el Estado le presta al ciudadano y a los empresarios a través de las Ventanillas Únicas de Comercio Exterior (ventanilla única), la simplificación de trámites de comercio a lo largo de toda la cadena de suministros; el uso de la factura electrónica, herramienta que disminuye la evasión de impuestos e incrementan la eficiencia empresarial; y los sistemas electrónicos de contratación pública que dan transparencia y democratizan las compras realizadas por el estado.

Se señala la importancia de incorporar mecanismos de firma electrónica y/o digital certificada, siguiendo el patrón de desarrollo de las Ventanillas Únicas ya consolidadas en la región y en el mundo, con hincapié en el uso de firma electrónica o digital para operar el sistema de manera más efectiva y segura (Sistema Económico Latinoamericano y del Caribe SELA, 2012).

Así también se hace un llamado a los gobiernos a propiciar a través de algún instrumento normativo supranacional el reconocimiento de las firmas electrónicas o digitales de cada país bajo sus leyes y normas. Un ejemplo de ello es el proyecto de reconocimiento de la ALADI para el sistema de certificación digital de origen, o el Federal Bridge Certification Authority que da validez a las firmas digitales emitidas en los diferentes ordenamientos jurídicos de los Estados Unidos (Sistema Económico Latinoamericano y del Caribe SELA, 2012).

Argentina, Ley 25506 del 2001 – Ley de Firma Digital Reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica.

Bolivia, Ley 080 de 2007 – Ley de Documentos, Firmas y Comercio Electrónico de 2007.

Esta ley reconoce el valor jurídico y probatorio de: i. Los actos jurídicos celebrados mediante medios electrónicos u otros de mayor avance tecnológico realizados por personas naturales, jurídicas, empresas colectivas o unipersonales, comunidades de bienes y otras entidades que constituyan una unidad económica sujeta a derechos y obligaciones, ii. El uso de firmas electrónicas debidamente certificadas por una Entidad de Certificación acreditada bajo lo estipulado en la presente ley, iii. Los actos civiles y comerciales que utilicen directa o indirectamente medios electrónicos u otros de mayor avance tecnológico para realizar actividades del comercio electrónico.

Brasil, Decreto Ley 3.996 de 2001 y Decreto Ley 4.414, de 2002. Regula la prestación del servicio de certificación digital de firma electrónica. Se ha intentado promover proyectos en materia de ley de comercio electrónico, pero el país considera suficiente la normativa existente en otras normas que han habilitado el uso de firma electrónica, además de contar ya con decretos en materia específica que regulan dicha prestación de servicio. Brasil es un país de la región que se reconoce por la masificación efectiva del uso de firma electrónica avanzada, exigiendo su uso en materia tributaria.

Chile, Ley 19.799 de 2002 - Ley de Documentos Electrónicos La ley adopta las disposiciones relativas a los documentos electrónicos, firmas electrónicas y servicios de certificación de las firmas.

Colombia, Ley 527 de 1999. Ley de Validez Jurídica y Probatoria de los mensajes de datos.

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones. Colombia ha desarrollado infinidad de habilitantes normativos que han permitido ir abonando un camino hacia la masificación.

Costa Rica, Ley 8454 de 2005 - Ley de certificados, firmas digitales y documentos electrónicos

Establece el marco jurídico general para la utilización segura de los documentos electrónicos y la firma digital en las entidades públicas y privadas

Cuba, En Cuba no existe una legislación especial que regule el comercio electrónico, sin embargo existen normas que habilitan su uso en diferentes disciplinas del derecho.

México, Ley de Firma Electrónica Avanzada de 2012. Corresponde a una nueva Ley de Comercio Electrónico que incluye modificaciones al Código Civil y otras leyes que le dan marco jurídico a la firma electrónica. Regula el uso de la firma electrónica avanzada en los actos previstos en la Ley y la expedición de certificados digitales, servicios relacionados con la firma electrónica avanzada y su homologación.

Paraguay, La reglamentación de la Ley Nº 4017/10, "De validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico", a través del decreto Nº 7.369. Este decreto especifica aspectos como la reproducción de documentos originales por medios electrónicos, la digitalización de archivos públicos, así como la certificación de los documentos y requisitos para su aplicación. En cuanto al servicio de archivo y conservación de documentos y datos en mensajes de datos, el decreto enuncia que las entidades que realicen la reproducción de documentos originales por medios electrónicos o que presten los servicios de almacenamiento deben incorporar un procedimiento estampado que garantice los efectos del documento electrónico. Esto equivale al documento físico que almacena.

Perú, Ley No. 27269 de 2000 – Ley de Firmas y Certificados Digitales Regula la utilización de la Firma Electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve una manifestación de la voluntad.

Uruguay, Ley 18.600 de 2009 – Ley de Documento electrónico y firma electrónica.

Esta Ley reconoce la admisibilidad, validez y eficacia jurídica del documento electrónico y de la firma electrónica.

Venezuela, Decreto Ley Nº 1204 de 2001, Ley de Mensajes de Datos y Firmas Electrónicas

El Decreto Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas

naturales o jurídicas, públicas o privadas, así como regula todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos. (Sistema Económico Latinoamericano y del Caribe SELA, 2012, págs. 15,16,17,18,19)

España, la Ley 59/2003 regula la firma electrónica, su eficacia jurídica y la prestación de los servicios de certificación. En el marco de las directivas de la Unión Europea, el Estado español ha aprobado un conjunto de medidas legislativas, como la Ley de Firma Electrónica y el RD sobre el Documento Nacional de Identidad electrónico, para la creación de instrumentos capaces de acreditar la identidad de los intervinientes en las comunicaciones electrónicas y asegurar la procedencia y la integridad de los mensajes intercambiados.

La Comisión Europea el 4 junio de 2012 aprueba un reglamento para hacer posible la firma electrónica transfronteriza, basándola en los medios que más garantías ofrecen; es decir, los DNI electrónicos de los diferentes países europeos para facilitar la movilidad de los ciudadanos europeos entre los estados miembros, dando un impulso y más valor al DNI electrónico.

1.2.7 Firma Digital y firma electrónica en el Ecuador

La (Ley de Comercio Electrónico, Mesaje de Datos y Firma Eléctrónica, 2002) en el Art. 13 define a la Firma electrónica como “Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos”

En el cuerpo de la Ley de Comercio Electrónico, Mensaje de Datos y Firma Electrónica, se hace referencia únicamente al término "Firma Electrónica", mientras que en el Reglamento General a ésta misma Ley, en el artículo 15, se menciona, el término de "Firma Digital” y en ninguna parte se menciona el concepto de ésta última.

La firma electrónica permite la transacción segura de documentos y operaciones en aplicaciones computacionales garantizando los siguientes aspectos:

- Identidad, reconoce unívocamente a un emisor como autor del mensaje.
- Integridad, el documento no puede ser alterado de forma alguna durante la transmisión.

- No repudio, el emisor no puede negar en ningún caso que un documento no fue firmado.
- Confidencialidad, solo las partes autorizadas pueden leer el documento (si fuera el caso).

1.2.8 La Dirección General de Registro Civil, Identificación y Cedulación

La Dirección General de Registro Civil, Identificación y Cedulación es una entidad pública creada mediante Registro Oficial No.1252 el 29 de octubre de 1900 por el Presidente Constitucional de la República, General Eloy Alfaro Delgado que planteó al Congreso Nacional de la época un Proyecto de Ley de Registro Civil, actualmente tiene 113 años de vida institucional y se encuentra adscrita al Ministerio de Telecomunicaciones y de la Sociedad de la Información.

La misión de la DIGERCIC es: Realizar la identificación integral de los habitantes del Ecuador, registrar sus actos civiles y otorgar documentos seguros y confiables, garantizando la custodia y manejo adecuado de la información.”

1.2.9 Infraestructura de la DIGERCIC - Análisis de la Situación Actual

La DIGERCIC actualmente mantiene el sistema de identificación nacional conocido con MAGNA, además cuenta con un Sistema Automatizado de Identificación de Huellas Dactilares – AFIS (Automated Fingerprint Identification System) y para la consulta de información con instituciones externas tiene implementado un sistema WEB Services.

La DIGERCIC cuenta con dos centros de datos: principal en la ciudad de Guayaquil en la agencia Centro donde se encuentra instalado el nuevo sistema MAGNA, sistema AFIS y el sistema Web Services. En la ciudad de Quito en la agencia matriz se encuentra el centro de datos secundario donde se encuentra operando el centro de digitalización y los backup de los sistemas.

Las agencias provinciales y cantonales de la DIGERCIC se conectan a los sistemas a través de su red nacional de datos, actualmente existen 50 agencias conectadas al nuevo sistema magna de ellas 33 son mega agencias y 10 agencias cantonales modernizadas (Dirección General de Registro Civil, Identificación y Cedulación, 2013).

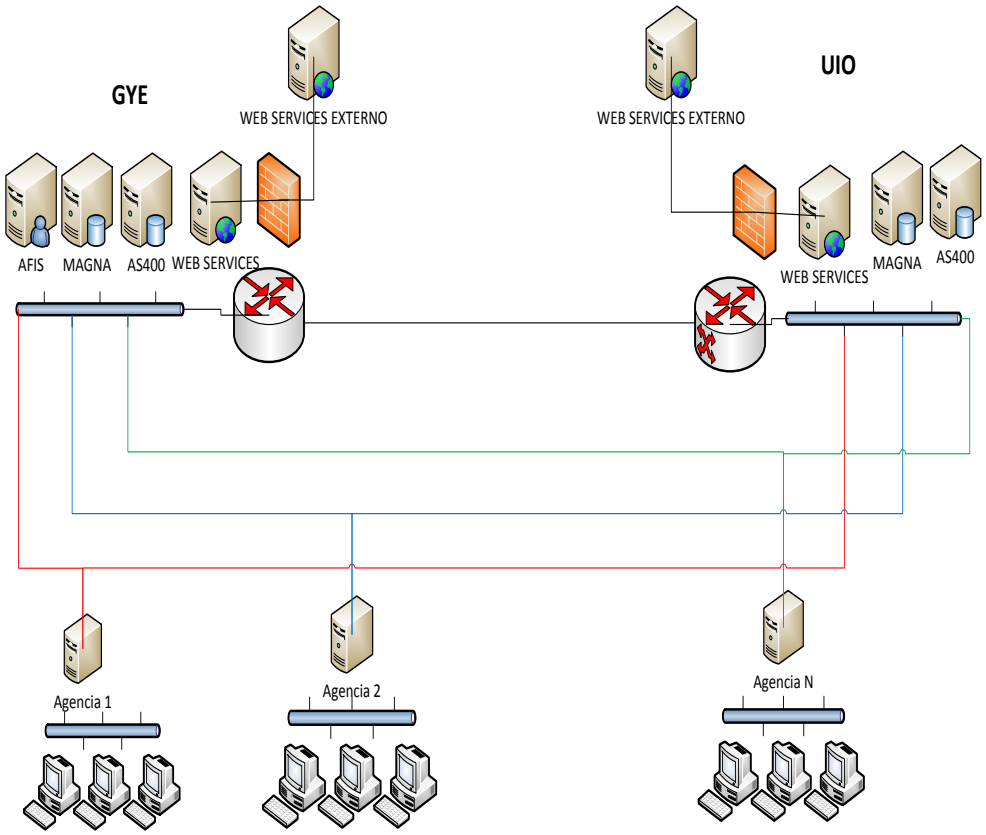


Figura 1. Esquema Red DIGERCIC

1.2.9.1 Sistema Magna

El sistema Magna es una plataforma de software personalizable para el registro de la población basada en la Web y la producción, emisión de documentos de identificación nacional como DNI, pasaporte electrónico, Visa de forma rápida y sencilla. Debido a su diseño basado en la web, Magna permite una integración con sistemas antiguos. Magna sirve como una herramienta integral que permite un fácil seguimiento y control de la totalidad de los procesos que suelen participar en las soluciones de extremo a extremo. (OTI - ON TRACK INNOVATIONS LTD, 2013)

1.2.9.1.1 Magna - Capas, Arquitectura Modular

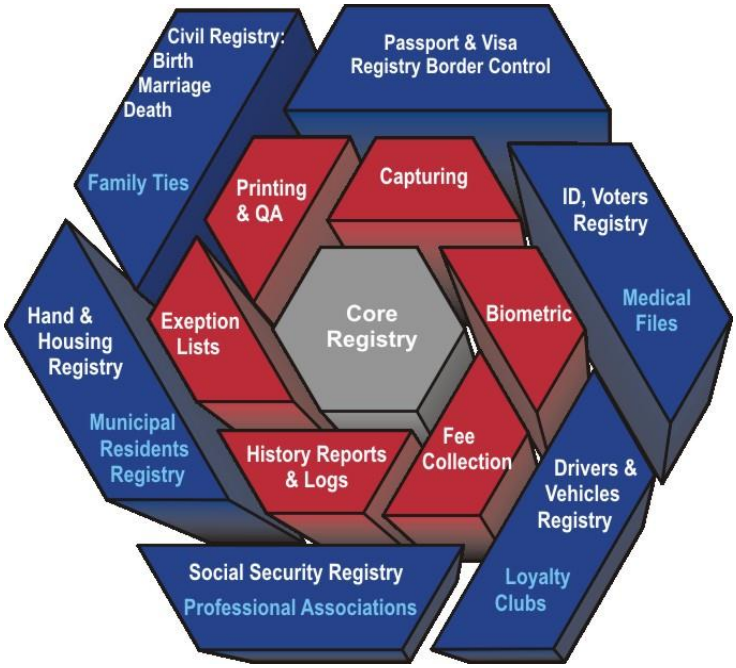


Figura 2. Arquitectura Magna

Fuente: (OTI - ON TRACK INNOVATIONS LTD, 2013)

La arquitectura de Magna se basa en una infraestructura jerárquica y modular, lo que permite planificar fácilmente la implementación de programas extensibles a largo plazo.

La arquitectura se compone de las siguientes capas:

Core Registro Layer (capa gris): Esta capa sirve como la capa central del Registro que se encuentra en cada implementación basada en Magna y el apoyo a todas las capas externas Magna.

Utilidades capa Común (capa roja): Esta capa se compone de una serie de utilidades / servicios generales, que se utilizan comúnmente en diversas aplicaciones. Por ejemplo, una utilidad de captura / inscripción se utiliza en la mayoría de los programas nacionales de identidad, pasaportes, licencias de conducir, Visas y mucho más. Al ser una utilidad común, que permite a los clientes reutilizar en futuras implementaciones con pequeñas adaptaciones (OTI - ON TRACK INNOVATIONS LTD, 2013).

Aplicaciones Layer (capa azul): Esta capa incluye varias aplicaciones que son compatibles con las capas anteriores. Estas aplicaciones no tienen que implementarse

todas a la vez, y se pueden añadir una a la vez, según sea necesario, la utilización de los servicios públicos existentes.

Con el sistema MAGNA se puede:

- Implementar un sistema de registro de población / cliente del estado de la técnica modular, coexistiendo con los sistemas existentes.
- Migrar de un sistema técnicamente complicado a uno fácil de usar, que permite una respuesta rápida a la nueva legislación, los reglamentos, reglas de negocio y los procedimientos de trabajo.
- Prestar servicios de administración electrónica en línea que permiten la ejecución de aplicaciones.
- Implementar sistemas de expedición de documentos de registro y evolutivos y robustos.
- Garantizar la calidad e integridad de la información de base de datos de registro.

Magna proporciona mejora de los servicios gubernamentales, la introducción de soluciones de escalabilidad y reducir el tiempo necesario para la implementación del sistema de registro. El sistema es a prueba de manipulaciones y resistente a falsificaciones, facilita adaptaciones incluso sin conocimientos técnicos a través de una interfaz gráfica de usuario avanzada (GUI) y ofrece una arquitectura genérica innovadora con una función de herramientas de personalización.

Alcance Magna

Magna normalmente se compone de los siguientes sub-sistemas (módulos):

- Magna Inscripción - Responsable de la inscripción de los datos y la transferencia a una base central de datos demográficos y biométricos personales.
- Magna Registro - Gestiona la creación y el manejo de la interfaz de la base de datos central con subsistemas biométricos (OTI - ON TRACK INNOVATIONS LTD, 2013).
- Magna Producción y personalización - Monitorea los documentos de la emisión y el proceso de personalización, mientras incrusta elementos de seguridad.

- Magna Documentos - Varias aplicaciones que validan la autenticidad de los documentos y de los titulares (control de fronteras, permisos de conducción, etc.).

Actualmente la DIGERCIC cuenta únicamente con el módulo de Registro Civil y licencias para el registro de nacimientos, matrimonios y defunciones con cobertura a nivel nacional.

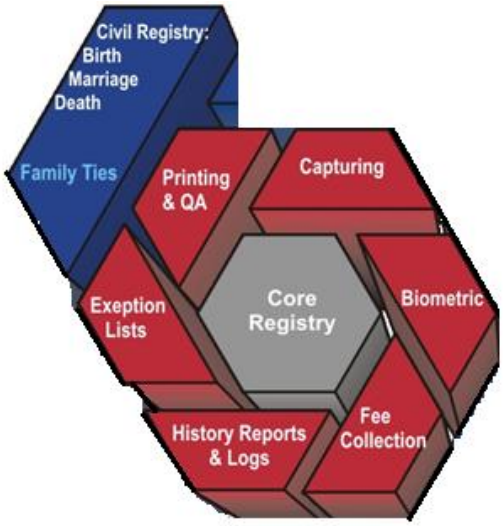


Figura 3. Arquitectura Magna- DIGERCIC

Fuente: (OTI - ON TRACK INNOVATIONS LTD, 2013)

1.2.9.1.2 Seguridades del Sistema Magna

Criptografía

El sistema Magna utiliza criptografía en tres áreas principales:

1. Para proteger los ordenadores y bases de datos y los datos en el sistema
    a) Cifrar todos los datos con lo que evita ser vulnerable al robo de información.
    b) Canales de comunicación Cifrados con red privada virtual (VPN)
    c) Cifra canales web mediante SSL
    d) Firma digital de los datos para asegurarse de que no se modifica en tránsito.
2. Para proteger el documento que se está creando contra la falsificación
    a) Cifrar datos y / o signos tales como huellas dactilares minucias

b) Implementar el cifrado y la firma de los datos tal como se define en los estándares para los pasaportes electrónicos y tarjetas de identidad electrónicos (OTI - ON TRACK INNOVATIONS LTD, 2013).

3. En el marco de la utilización del documento durante su vigencia.

a) Utiliza certificados y criptografía incrustados en el chip para facilitar el comercio electrónico, la identificación remota y otras funciones de la administración electrónica.

1.2.9.1.3 Protección del sistema y los datos

Un sistema de registro típico se compone de muchos equipos que contengan datos y pueden ser transferirlos a otro: Central servidores de Uso y estaciones, servidores del sitio de recuperación de desastres y estaciones, estacionarios (fijos) y estaciones de enrolamiento / captura de móviles, etc.

Las estaciones de inscripción móviles y fijos fuera del Centro estarán protegidos mediante el cifrado de disco duro de la estación (AES-256). Será necesaria la autenticación de dos o tres factores para acceder al disco. Los datos que se mueven a partir de estas estaciones para el centro también se cifrarán utilizando cifrado: AES-256, si los datos se transfieren en los medios de comunicación o VPN si los datos se transmiten por la red. Conexiones de servidor Web se pueden proteger con SSL (OTI - ON TRACK INNOVATIONS LTD, 2013).

1.2.9.1.4 Protección de documentos

Códigos de barras 2D son medios comunes para llevar a datos biométricos en un documento si un chip no está disponible. El uso típico de la criptografía es para cifrar y / o firmar el contenido de un código de barras 2D, cuando este es el medio para almacenar los datos biométricos, tales como las minucias de huellas dactilares.

Para documentos electrónicos, tales como pasaporte electrónico o Documento Nacional de Identificación electrónico - DNIe, la criptografía es un componente obligatorio se define en las normas para estos documentos. Sujeto a la autenticación pasiva, autenticación activa, control de acceso básico y extendido, Emisor y los certificados de usuario final son compatibles en nuestros sistemas de acuerdo con la Organización de Aviación Civil Internacional OACI, Unión Europea, o las normas locales.

1.2.9.1.5 Uso de documentos

Los documentos con información biométrica en los códigos de barras 2D pueden ser utilizados para verificar la identidad del titular en el momento de uso, por ejemplo, en la cabina de votación, en la presentación de la identificación de un agente de policía o a un empleado de banco, o en un puesto de control fronterizo .

La criptografía en los documentos electrónicos permite que los utilicemos de manera ventajosa en varios escenarios, que dependen de la identificación de la persona con rapidez y precisión:

1. Para el tránsito seguro y rápido de control de fronteras y puertas de seguridad en aeropuertos
2. Para la identificación de la persona a distancia para las transacciones basadas en Internet.
3. Para la firma de los documentos por los ciudadanos, de acuerdo con las leyes vigentes "firma electrónica".
4. Por diversas transacciones cubiertas genéricamente bajo el nombre de "administración electrónica (o eGOV)" - diversos servicios gubernamentales, que sólo se pueden dar después de identificar al ciudadano (OTI - ON TRACK INNOVATIONS LTD, 2013).

1.2.9.1.6 Infraestructura de Clave Pública (PKI)

Infraestructura de Clave Pública (PKI) es una necesidad de recursos comunes en muchos de los proyectos que tienen chip electrónico en el documento. La PKI incluye Autoridades de Certificación (AC), Autoridades de registro e interfaces que permiten que el sistema utilice estas herramientas.

La PKI utiliza módulos de seguridad de hardware (HSM) para mantener toda la información de clave privada/secreta y realizar operaciones criptográficas como exige diferentes clientes criptográficos. Las autoridades de certificación presentan certificados para las estaciones emisoras, operadores de estaciones de trabajo, los puntos de verificación de pasaportes y hasta los usuarios finales.

Magna es compatible con todos los usos antes mencionados de la criptografía, personalizados según sea necesario para cada país y proyecto específico (OTI - ON TRACK INNOVATIONS LTD, 2013).

1.2.9.1.7 Cédula electrónica

El Documento de Identidad Nacional (DIN) ó cédula de identidad, como tradicionalmente se lo ha denominado en el Ecuador, es el que debe permitir identificar y verificar que un ciudadano es quien dice ser, de manera ágil y segura y además le da acceso a la persona a todos sus derechos como ciudadano (Dirección General de Registro Civil, Identificación y Cedulación, 2010, pág. 6).

En función de su tipo de uso y el marco legal el Documento de Identidad Nacional - DIN evoluciona y pasa por las siguientes fases:

1. Documento de Identidad Nacional Tradicional (Cédula de Identidad).- Es una tarjeta que solo tiene información impresa de los datos del ciudadano y buscaba identificarlo a través de su foto, firma o imagen de su huella dactilar. Este documento no asegura que el que lo porta es la persona que dice ser y además con una inversión relativamente barata se lo puede falsificar.
2. Documento de Identidad Nacional electrónico - eDNI.- Además de la información impresa, contiene un chip con información digital encriptada del ciudadano y parte de su información biométrica, como puede ser huellas digitales o la foto del ciudadano. A partir de esta información se puede identificar al ciudadano y establecer que quien porta el documento es quien dice ser. Adicionalmente este tipo de documentos contienen certificados digitales que garantizan la inviolabilidad de la información.
3. Documento de Identidad Nacional electrónico con Firma Electrónica.- Es una evolución del eDNI (Dirección General de Registro Civil, Identificación y Cedulación, 2010) que permite que el ciudadano pueda además firmar documento a partir del documento de identidad y establecer otros servicios electrónicos de manera segura (Dirección General de Registro Civil, Identificación y Cedulación, 2010, pág. 19).

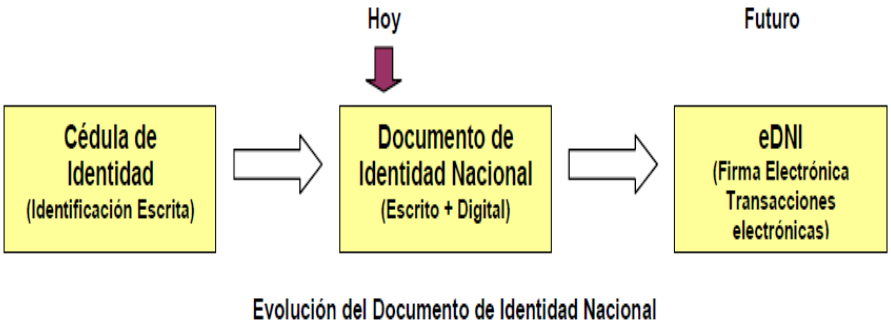


Figura 4. Evolución DNI

Fuente: (Dirección General de Registro Civil, Identificación y Cedulación, 2010)

"A pesar de que el actual DIN ecuatoriano contiene un Chip no puede considerárselo como un eDNI hasta que el Certificado Electrónico que contiene sea autorizado por el ente regulador de acuerdo a la Ley de Comercio Electrónico, Firma Electrónica y Mensajes de Datos hoy vigente en el Ecuador" (Dirección General de Registro Civil, Identificación y Cedulación, 2010, pág. 18).

"La capacidad del nuevo DIN permitirá eliminar muchos papeles y copias que hoy se exigen para trámites en diferentes instituciones, adicionalmente provocará que servicios que no agregan valor a la identidad del ciudadano y que por el contrario están sujetos a ser falsificados, como son los múltiples certificados que hoy se exigen, se dejen de dar en las oficinas de atención al ciudadano del Registro Civil" (Dirección General de Registro Civil, Identificación y Cedulación, 2010, pág. 18).

1.2.9.1.8 Especificaciones

El nuevo Documento de Identidad Nacional en el Ecuador contiene información física y electrónica. En el caso de la información electrónica, la misma se almacena en un Chip libre de contacto (Tecnología de Radio Frecuencia - RFID).

Información en el Chip.- Además de la información impresa, conforme Al estándar internacional ICAO 9303 para documentos de viaje, contiene un chip con información digital encriptada del ciudadano incluyendo información biométrica (huellas digitales y la foto del ciudadano).

A partir de esta información se puede identificar al ciudadano y establecer que quien porta el documento es quien dice ser.

El chip no está expuesto a simple vista, está embebido en el interior del plástico, según la norma internacional ISO 14443 B para tarjetas de identificación con circuito integrado libre de contacto (tarjetas de proximidad). Su capacidad de almacenamiento actual es de 66 Kilobytes, la cual se irá ampliando en la medida de la disponibilidad, compatibilidad y costos (Dirección General de Registro Civil, Identificación y Cedulación, 2010).

En resumen, a continuación las especificaciones de la cédula electrónica:

- ICAO 9303
- ISO 14443B
- Libre de contactos (Contact Less)
- Identificación por Radiofrecuencia (RFID), alcance hasta 5 cms.
- Frecuencia de operación 13.56 MHz
- Capacidad disponible de almacenamiento de información 66 Kbyte
- Sistema operativo propietario Hércules (OTI)
- Cifrado DES de alta seguridad, requiere de chip Secure Access Module (SAM)
- Norma ISO 7816 para el SAM
- Código de fábrica Chip Serial Number (CSN) de 8 bytes 64 bits

Actualmente la información en el Chip se graba y luego se cierra para que no pueda ser agregada más información. Sin embargo se está considerando cambiar esta definición y migrar de una solución propietaria a una que cumpla con estándares internacionales abiertas de modo que solo la información confidencial quede cerrada y se pueda utilizar el espacio remanente para nueva información abierta que puede ser actualizable inclusive; permitiendo la incorporación de nuevas aplicaciones que incrementen la usabilidad de la cédula (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2011).

La segunda versión de cédula (con ID File) ha sido implementada con el objetivo de permitir acceso abierto de cierta información, manteniendo la seguridad ICAO de los datos del ciudadano (Dirección General de Registro Civil, Identificación y Cedulación, 2010).

En la primera versión de cédula electrónica el chip contiene la siguiente información:

Tabla 1.

Información Chip Cédula

NO.	GRUPO	DATO	COMENTARIO
1	DG1	Número de Cédula (Identificación) de la persona	
2	DG1	Número del Documento	Número único que identifica a la tarjeta.
3	DG1	Fecha de Expiración de la tarjeta	
4	DG1	Apellidos de la persona	Ajustado en el espacio definido en el estándar. En el grupo DG11 están los apellidos completos.
5	DG1	Nombres de la persona	Ajustado en el espacio definido en el estándar. En el grupo DG11 están los apellidos completos.
6	DG1	Sexo de la persona	
7	DG1	Código de la Nacionalidad de la persona	
8	DG1	Fecha de Nacimiento	
9	DG1	Estado de la emisión del documento	
10	DG2	Foto digitalizada de la persona	
11	DG3	Número del dedo para la huella digital 1	
12	DG3	Huella Digital 1	
13	DG3	Número del dedo para la huella digital 2	
14	DG3	Huella Digital 2	
15	DG7	Firma digitalizada de la persona	
16	DG11	Lugar de Nacimiento	Si es en el Ecuador en formato: Provincia, Cantón y Parroquia. Si es en el exterior en formato: País y Ciudad.
17	DG11	Profesión u Ocupación de la persona	
18	DG11	Número de teléfono de la persona	
19	DG11	Número celular de la persona	
20	DG11	Dirección de domicilio de la persona. Información principal.	Si es en el Ecuador en formato: Provincia, Cantón y Parroquia. Si es en el exterior en formato: País y Ciudad.
21	DG11	Dirección de domicilio de la persona. Primera línea de información.	
22	DG11	Dirección de domicilio de la persona. Segunda	
23	DG11	Dirección de domicilio de la persona. Tercera línea de información.	
24	DG11	Apellidos de la persona	Información completa
25	DG11	Nombres de la persona	Información completa
26	DG11	Clave pública de autenticación active	
27	DG11	Código del Chip	

Fuente: (Dirección General de Registro Civil, Identificación y Cedulación, 2010)

CAPÍTULO II

MARCO TEORICO Y CONCEPTUAL

2.1 MARCO TEÓRICO

Comunicar es el hecho de transmitir información significativa. Es la acción a través de la cual los individuos se relacionan entre sí.

Para que la comunicación se produzca se requieren tres elementos básicos: Un emisor, un mensaje y un receptor. A estos tres elementos fundamentales hay que sumarle dos factores de igual importancia: El código y el canal. Se les conoce como los factores de la comunicación.

Señales analógicas: Pueden ser representadas mediante funciones que toman un número infinito de valores en cualquier intervalo de tiempo considerado. Para transmitir señales analógicas se emplean sistemas de transmisión analógicos, y la información va contenida en la propia forma de onda (Estepa, 2004, pág. 39).

Señales digitales: Pueden ser representadas mediante funciones que toman un número finito de valores en cualquier intervalo de tiempo. Las señales digitales necesitarán sistemas de transmisión digitales donde la información estará contenida en los pulsos codificados, y no en la forma de onda (Estepa, 2004, pág. 39).

2.1.1 Criptografía

La criptografía es el estudio de los sistemas que hacen posible el proceso de encripción. La encripción es el proceso que se utiliza para hacer que una cierta información sea indescifrable para todo el mundo, excepto para las personas que conozcan la clave que le permitirá desencriptar la información (CYBSEC Security Systems, 2009).

2.1.2 Criptografía simétrica

La criptografía simétrica, es el conjunto de algoritmos que funcionan con una sola llave o clave, que tienen ambos lados de la comunicación y que debe de permanecer secreta (MathCon, sf), es decir se utiliza la misma clave para encriptar y desencriptar información. Algoritmos simétricos: DES, Blowfish, IDEA (International Data Encryption Algorithm).

2.1.3 Criptografía asimétrica

La criptografía asimétrica utiliza dos llaves, una pública y la otra privada. La llave pública es aquella a la que cualquier persona puede tener acceso, mientras que la llave privada es aquella que sólo la persona que la recibe es capaz de descifrar. Una de la claves se emplea para codificar, y la otra se usa para decodificar (Lucena López, 2007, pág. 172).

2.1.4 Sistemas de información y su clasificación

Un sistema de información (SI) es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad. Un sistema de información combina personas, datos, recursos y procesos. Todos estos elementos interactúan entre sí para procesar los datos (incluyendo procesos manuales y automáticos) dando lugar a información más elaborada y distribuyéndola de la manera más adecuada posible en una determinada organización en función de sus objetivos.

Los componentes básicos que constituyen un sistema de información son:

Datos: los cuales almacena, procesa y transforma para obtener como resultado final información, la cuál será suministrada a los diferentes usuarios del sistema.

Usuarios: personal directivo, empleados y en general cualquier agente de la organización empresarial que utilice la información en su puesto de trabajo.

Equipos: informáticos, software, hardware y tecnologías de almacenamiento de la información y de las telecomunicaciones.

En cuanto a los tipos de sistemas de información se tienen los siguientes:

- Sistemas de procesamiento de operaciones: sistemas informáticos encargados de la administración de aquellas operaciones diarias de rutina necesarias en la gestión empresarial.
- Sistemas de trabajo del conocimiento: encargados de apoyar a los agentes que manejan información en la creación e integración de nuevos conocimientos para la empresa.
- Sistemas de automatización en la oficina: empleados para incrementar la productividad de los empleados que manejan la información en los niveles inferiores de la organización.

- Sistemas de información para la administración: empleados en el proceso de planificación, control y toma de decisiones proporcionando informes sobre las actividades ordinarias.
- Sistemas para el soporte de decisiones: sistemas informáticos que ayudan a los distintos usuarios en el proceso de toma de decisiones,
- Sistemas de soporte gerencial: sistemas de información a nivel estratégico de la organización diseñados para tomar decisiones estratégicas, mediante el empleo de gráficos y comunicaciones avanzadas (Peña, 2006).

2.2 MARCO CONCEPTUAL

De acuerdo con la declaración de principios de la Cumbre Mundial sobre la Sociedad de la Información Cumbre de la Sociedad de la Información, llevado a cabo en Ginebra (Suiza) en 2003 los líderes mundiales declararon: "nuestro deseo y compromiso comunes de construir una Sociedad de la Información centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos".

Firma manuscrita

Se puede indicar que en Roma, los documentos no eran firmados. Existía una ceremonia llamada manufirmatio, por la cual, luego de la lectura del documento por su autor o el notarius, era desplegado sobre una mesa y se le pasaba la mano por el pergamino en signo de su aceptación. Solamente después de cumplir esta ceremonia se estampaba el nombre del autor (KRAFFT, 2002).

En el Sistema Jurídico Visigótico existía la confirmación del documento por los testigos que lo tocaban (chartam tangere), signaban o suscribían (firmatio, roboratio, stipulatio). La firma del que da el documento o librador es corriente, pero no imprescindible. Los documentos privados son, en ocasiones, confirmados por documentos reales. Desde la época euriciana las leyes visigodas prestaron atención a

las formalidades documentales, regulando detalladamente las suscripciones, signos y comprobación de escrituras (TOMAS & FRANCISCO, 1996, pág. 53).

La "subscriptio", representaba la indicación del nombre del signante y la fecha, y el "signum", un rasgo que la sustituye si no sabe o no puede escribir. La "subcriptio" daba pleno valor probatorio al documento y el "signun" debía ser completado con el juramento de la veracidad por parte de uno de los testigos. Si falta la firma y el signo del autor del documento, éste es inoperante y debe completarse con el juramento de los testigos sobre la veracidad del contenido.

En la Edad Media, la documentación regia viene garantizada en su autenticidad por la implantación del sello real. Sello que posteriormente pasó a las clases nobles y privilegiadas (TOMAS & FRANCISCO, 1996, pág. 54)

La firma es definida en la doctrina como el signo personal distintivo que, permite informar acerca de la identidad del autor de un documento, y manifestar su acuerdo sobre el contenido del acto (Cuervo, sf)

La Real Academia de la Lengua define la firma como: "nombre y apellido o título de una persona que ésta pone con rúbrica al pie de un documento escrito de mano propia o ajena, para darle autenticidad, para expresar que se aprueba su contenido o para obligarse a lo que en él se dice" (Cuervo, sf).

2.2.1 Comercio Electrónico

Según la Organización Mundial de Comercio en su programa de trabajo entiende por la expresión “Comercio Electrónico”, la producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos.

2.2.2 Firma digital.

La firma digital permite al receptor de un mensaje verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación. De este modo, la firma digital ofrece el soporte para la autenticación e integridad de los datos así como para el no repudio en origen, ya que el originador de un mensaje firmado digitalmente no puede argumentar que no lo es.

Una firma digital está destinada al mismo propósito que una manuscrita. Sin embargo, una firma manuscrita es sencilla de falsificar mientras que la digital es imposible mientras no se descubra la clave privada del firmante.

La firma digital se basa en la propiedad de un mensaje cifrado utilizando la clave privada de un usuario sólo puede ser descifrado utilizando la clave pública asociada. De tal manera, se tiene la seguridad de que el mensaje que ha podido descifrarse utilizando la clave pública sólo pudo cifrarse utilizando la privada. La firma digital, por tanto, es un cifrado del mensaje que se está firmando pero utilizando la clave privada en lugar de la pública.

La firma digital hace uso de funciones hash. Una función hash es una operación que se realiza sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado otro conjunto de datos, denominado resumen de los datos originales, de tamaño fijo e independiente del tamaño original que, además, tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es prácticamente imposible encontrar dos mensajes distintos que tengan un resumen (hash) idéntico (Moneda, sf).

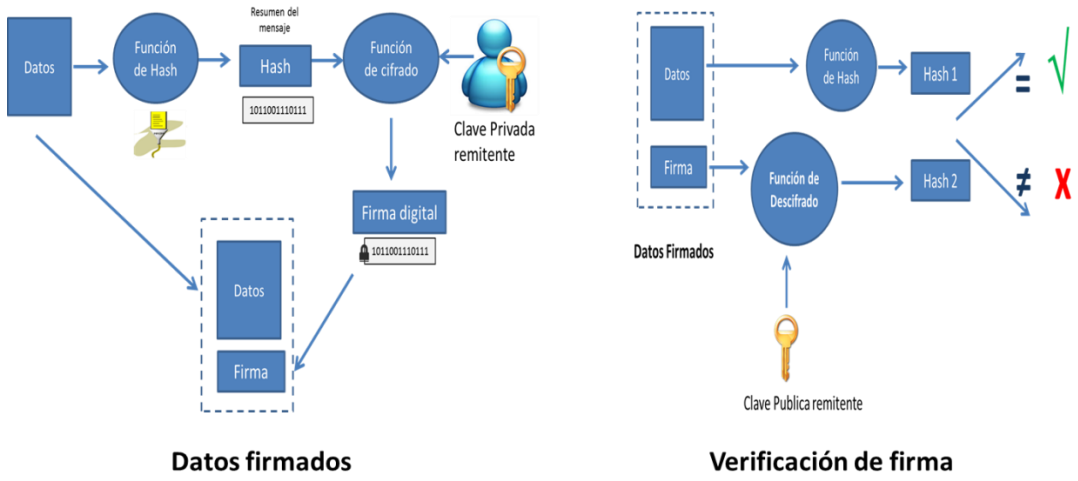


Figura 5. Firma Digital

Fuente: (AGESIC, Agencia de gobierno electrónico y sociedad de la informacion, sf)

2.2.3 Firma electrónica

"Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos" Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos Art. 13.

2.2.4 Certificado de firma electrónica

"Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad" Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos Art. 20.

La eficacia de las operaciones de cifrado y firma electrónica basadas en criptografía de clave pública sólo está garantizada si se tiene la certeza de que la clave privada de los usuarios sólo es conocida por dichos usuarios y que la pública puede ser dada a conocer a todos los demás usuarios con la seguridad de que no exista confusión entre las claves públicas de los distintos usuarios. Para garantizar la unicidad de las claves privadas se suele recurrir a soportes físicos tales como tarjetas inteligentes que garantizan la imposibilidad de la duplicación de las claves.

Por otra parte, para asegurar que una determinada clave pública pertenece a un usuario en concreto se utilizan los certificados digitales. Un certificado electrónico es un documento electrónico que asocia una clave pública con la identidad de su propietario.

La manera en que se puede confiar en el certificado de un usuario con el que nunca hemos tenido ninguna relación previa es mediante la confianza en terceras partes.

2.2.5 Infraestructura de llaves públicas (PKI)

Una infraestructura de llaves públicas es un sistema de entrega de certificados y llaves criptográficas lo cual hace posible la seguridad en transacciones económicas financieras y el intercambio de información sensible entre personas relativamente

desconocidas. Un PKI provee privacidad, control de acceso, integridad, autenticación y soporte para el no repudio en aplicaciones informáticas y transacciones de comercio electrónico. Un PKI administrará la generación y distribución de llaves públicas y privadas; y publicará las llaves públicas con la identificación de los usuarios en tablas electrónicas públicas (es decir servicios de directorio x.500). PKI provee un alto grado de confianza, manteniendo las claves privadas seguras, las claves públicas se conectan a sus respectivas claves privadas, y el par de claves públicas y privadas aseguran la veracidad de la persona quien dice ser (ONGEI, Oficina Nacional de Gobierno Electrónico e Informatica, 2002).

Actualmente la construcción de la infraestructura de llave pública es uno de los aspectos más importantes en las aplicaciones criptográficas, especialmente en la interconexión de la Internet y los dispositivos móviles.

2.2.6 Componentes PKI

La Infraestructura de Llave Publica (PKI) es una combinación de software, tecnologías de cifrado, y servicios que permiten proteger la seguridad de las transacciones de información en un sistema distribuido. PKI integra certificados digitales, criptografía de llave pública y autoridades de certificación en una arquitectura de seguridad.

Un Certificado Digital es un documento que vıncula una llave pública con una entidad final y que es firmado por una autoridad certificadora para demostrar su validez e integridad. A continuación y como se indica en el gráfico N° 6, se listan los componentes fundamentales que conforman la Infraestructura de Llave Publica (PKI) (Martínez, 2005, pág. 42):

2.2.6.1 Entidad final

Es el termino genérico para denotar a los usuarios finales o cualquier entidad que pueda ser identificada (personas, servidores, compañías, etc.) mediante un certificado digital expedido por una Autoridad Certificadora.

2.2.6.2 Autoridad Certificadora (AC)

La AC es la entidad que expide los certificados digitales, así como también la lista de revocación (CRL). Adicionalmente puede soportar funciones administrativas, aunque generalmente estas son delegadas a una o varias.

2.2.6.3 Autoridades de Registro

Autoridad de Registro (AR). Una AR es componente opcional que puede asumir funciones administrativas de la CA. Las funciones de la AR están frecuentemente asociadas con la afiliación de las entidades finales, pero adicionalmente puede asistir en otras áreas.

2.2.6.4 Repositorio.

El repositorio es el término genérico utilizado para denotar cualquier método para almacenamiento de certificados y listas de revocación (CRLs) que permita el acceso por parte de las entidades finales a dichos documentos.

2.2.6.5 Emisor CRL

El emisor CRL es un componente opcional el cual puede ser utilizado por una AC para delegar las tareas de publicación de las listas de revocación.

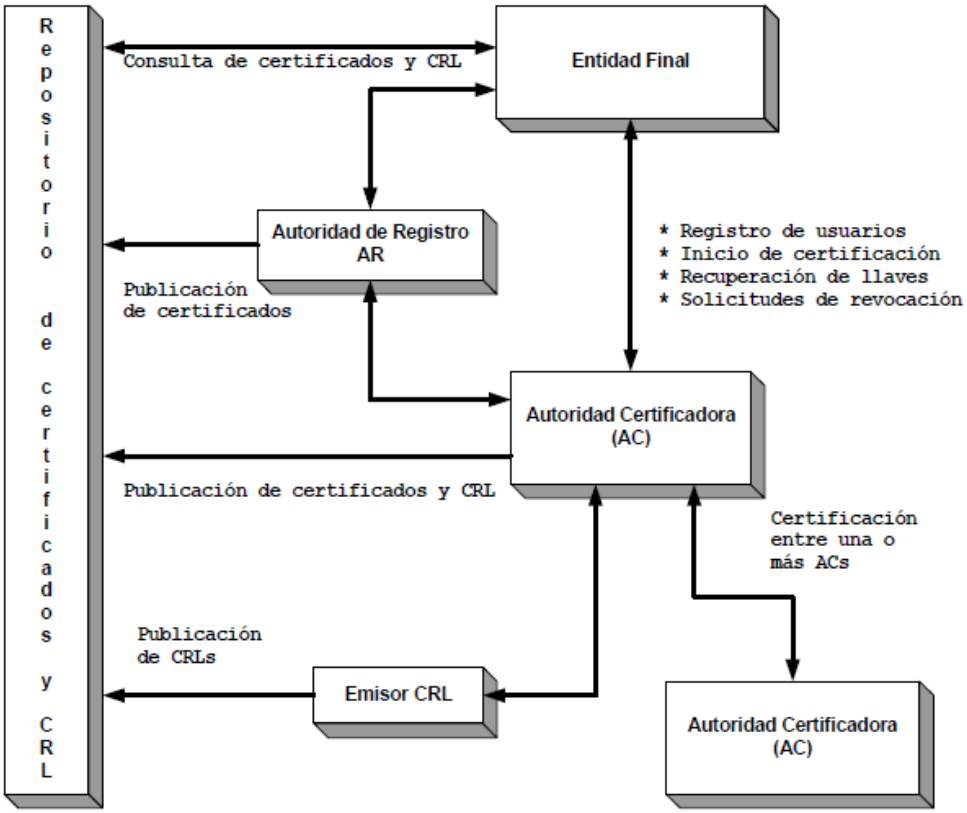


Figura 6. : Componentes PKI

Fuente: (Martínez, 2005)

2.2.7 Autoridades Certificadoras (ACs)

Una Autoridad Certificadora, es el componente fundamental de la infraestructura de llave pública. Es una combinación de hardware, software, y personas que conforman una arquitectura de seguridad. La AC es conocida por sus dos atributos más importantes: su llave publica y su nombre o identificador.

La AC expide certificados de llave pública para cada entidad, confirmando plenamente la identidad del suscriptor con sus respectivos documentos de identidad. Un certificado digital incluye la llave pública, información acerca de la identidad del suscriptor que posee la llave privada, un periodo de validez del certificado, y la firma digital de la propia autoridad certificadora. El certificado puede contener otros campos como por ejemplo: información adicional sobre la autoridad certificadora o información acerca de usos recomendados para la llave pública. Un suscriptor es un individuo o entidad de negocio que ha contratado a una AC para recibir un

certificado digital el cual le permita verificar su identidad para transacciones firmadas digitalmente.

Una AC también debe de expedir y procesar listas de revocación de certificados

(CRLs), las cuales son listas de los certificados que han sido invalidados. Los certificados pueden ser revocados por distintas razones, por ejemplo, si un propietario ha perdido su llave privada; la compañía que posee el certificado cambia de nombre; o simplemente el propietario de la llave privada abandona la empresa para la cual trabaja. Las CRLs también deben de documentar el estado de revocación de los certificados; al igual que el periodo de validez de un certificado digital, la lista de revocación debe de especificar la fecha exacta en la cual el certificado fue revocado.

Una Autoridad Certificadora desempeña cuatro funciones básicas en PKI:

•Expedición de certificados digitales.

•Expedición de listas de revocación.

•Publicación de sus certificados digitales y su lista de revocación.

•Almacenamiento del estado de los certificados expirados que ha expedido.

Estos cuatro requerimientos son difíciles de satisfacer simultáneamente. Para cumplir con estos requerimientos, una AC puede delegar ciertas funciones a otros componentes de la infraestructura.

Una AC puede expedir certificados a usuarios, a otras ACs, o a ambos. Cuando una AC expide un certificado, está asegurando que el sujeto (la entidad nombrada en el certificado) posee la llave privada que corresponde a la llave pública contenida en el certificado digital. Si la AC incluye información adicional en el certificado, la AC esta también afirmando que la información corresponde a la misma entidad. Esta información adicional puede ser una dirección de correo electrónico, o información de políticas para el tipo de aplicaciones en las cuales puede ser utilizada la llave pública.

Cuando el sujeto del certificado es otra AC, el emisor está afirmando que los certificados de la otra AC son de confianza (Martínez, 2005, págs. 44,45).

La AC inserta su nombre en cada certificado y CRL que genera, y los firma con su llave privada. Una vez que los usuarios establecen que confían en la AC

(directamente, o a través de una ruta de certificación) ellos pueden confiar en los certificados expedidos por dicha AC. Los usuarios fácilmente pueden identificar los certificados expedidos por la AC simplemente por la comparación del nombre. Para asegurar que el certificado es genuino, ellos pueden verificar la firma utilizando la llave pública de la AC. Como resultado, es extremadamente importante que la AC brinde una protección adecuada para su propia llave privada (Martínez, 2005, pág. 45).

2.2.8 Autoridad de Registro (AR)

Una AR es diseñada para verificar el contenido de un certificado para la AC. El contenido del certificado puede reflejar información proporcionada por una tercera parte. Por ejemplo, el límite de crédito asignado a una tarjeta de crédito refleja la información obtenida del buró de crédito. La AR conjunta estos datos de entrada y proporciona la información de una forma digerida a la AC.

Cada AC mantiene una lista de las ARs acreditadas; es decir, las ARs que son confiables. Una AR es conocida por la AC por su nombre y llave pública. Mediante la verificación de la firma digital de la AR una AC puede estar segura que la AR es una entidad acreditada. Al igual que una AC, la AR debe de tener un cuidado extremo en la protección de su llave privada.

2.2.9 Repositorio

El término repositorio es frecuentemente asociado con un directorio, pero este no es necesariamente el caso. En el contexto de PKI, un repositorio es un término genérico usado para denotar cualquier método para almacenamiento y recuperación de información referente a PKI tal como los certificados de llave pública y las CRLs. Un repositorio puede estar basado en la especificación X.500 con acceso para clientes a través de (Lightweight Directory Access Protocol) (LDAP), o incluso puede estar basado en algo mucho más sencillo como la descarga de un archivo plano de un servidor remoto vía FTP, o HTTP (Martínez, 2005, pág. 46).

El grupo de trabajo IETF PKIX 4 se ha dedicado al desarrollo de protocolos operacionales para facilitar la distribución de certificados de llave pública y CRLs, incluyendo LDAP, HTTP, y FTP.

También es posible delegar ciertas funciones de los sistemas del cliente a terceras partes confiables. Por ejemplo, el protocolo OCSP 5 (Online Certificate Status Protocol [RFC2560], http://www.ietf.org/rfc/rfc2560.txt) puede ser usado para preguntar a una tercera parte acerca del estado de revocación de uno o más certificados.

En cualquier caso, el funcionamiento clave del repositorio es que las entidades finales tengan algún mecanismo para obtener información de certificados y CRLs, o en otro caso que sean capaces de solicitar que esta tarea sea realizada en su representación.

2.2.10 Emisor CRL

El emisor CRL tal como su nombre lo dice, es el encargado de emitir la lista de revocación. Típicamente la AC que expide los certificados es también la responsable de expedir la lista de revocación asociada con esos certificados. Sin embargo, es posible para una AC delegar esa funcionalidad a otra entidad.

Entidades Finales

Las entidades finales PKI son organizaciones o individuos que usan PKI, pero no emiten certificados. Las entidades dependen de otros componentes PKI para obtener certificados, y para verificar certificados de otras entidades.

Las entidades finales algunas veces se confunden con usuarios finales. A pesar que frecuentemente este es el caso, el término entidad final significa algo bastante más genérico. Una entidad final puede ser un usuario final, un dispositivo como un ruteador o un servidor, incluso una AR o cualquier entidad que pueda ser identificado en el nombre del sujeto de un certificado de llave pública (Martínez, 2005, pág. 47).

Las entidades finales están ligadas a los certificados, y ´estas deben de inscribirse a la infraestructura de llave pública antes que puedan participar como miembros PKI (Martínez, 2005).

2.2.11 Arquitecturas PKI

Las entidades finales de PKI pueden obtener certificados de diferentes ACs, dependiendo de la organización o comunidad en la cual ellos son miembros. Una PKI esta típicamente compuesta de muchas ACs vinculadas por “rutas de confianza”.

Una ruta de confianza conecta a un componente confiable con una o más terceras partes confiables, de tal forma que todas las partes puedan tener confianza en la validez de un certificado (Martínez, 2005). Un destinatario de un mensaje firmado, el cual no tiene relación con la AC que emitió el certificado del remitente puede aún validar el certificado del remitente mediante una ruta entre su respectiva AC y la que expidió el certificado. Es importante resaltar que los usuarios finales confían en sus respectivas ACs que a su vez también confían en otras ACs, de aquí el término de "ruta de confianza".

El reto inicial es el despliegue de la infraestructura de llave pública de tal forma que pueda ser utilizada a través de empresas o agencias gubernamentales. Existen dos arquitecturas PKI tradicionales las cuales permiten alcanzar esta meta, las arquitecturas jerárquica y de malla. Más recientemente, varias empresas están buscando vincular sus propias PKIs con las de sus socios de negocio. Un tercer método, la arquitectura de puente está siendo desarrollada para atacar este problema. Estas tres arquitecturas son descritas en los párrafos siguientes.

2.2.11.1 Jerárquica:

Las Autoridades son organizadas jerárquicamente bajo una AC raíz la cual expide certificados a las ACs subordinadas. Estas ACs pueden expedir certificados a las ACs y/o usuarios de nivel inferior a su jerarquía. En el modelo jerárquico de PKI, cada parte conoce la llave pública de la AC de nivel superior (Martínez, 2005, pág. 48).

Cualquier certificado puede ser verificado a través de la ruta de certificación establecida entre la AC subordinada y la AC raíz. En el siguiente gráfico se muestra un ejemplo de la arquitectura jerárquica donde Alicia trata de validar el certificado de Benito. El certificado de Benito fue emitido por la AC4, el certificado de la AC4 a su vez fue expedido por la AC2, y finalmente el certificado de la AC2 fue emitido por la AC1 (la AC raíz), cuya llave pública es conocida por la AC de Alicia permitiéndole así verificar el certificado de Benito.

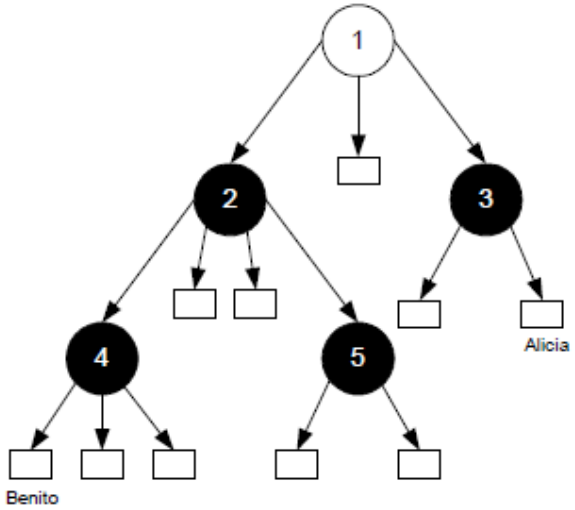


Figura 7. Arquitecturas PKI- Infraestructura Jerárquica

Fuente: (Martínez, 2005)

2.2.11.2 Malla:

En este esquema las ACs se certifican una con otra, resultando en una malla de relaciones de confianza entre las ACs. En el siguiente gráfico ilustra un ejemplo de la arquitectura de malla donde Alicia trata de verificar el certificado de Benito. Alicia conoce la llave pública de la AC3, mientras Benito conoce la llave pública de la AC4. Existen diversas rutas de certificación que pueden tomarse para llegar de Benito a Alicia; a continuación se explica la ruta más corta. El certificado de la AC4 fue expedido por la AC5 y finalmente el certificado de la AC5 fu expedido por la AC3. La AC3 es la misma AC que expidió el certificado de Alicia por lo cual ella conoce su llave pública la cual le permite realizar la tarea de verificación (Martínez, 2005, pág. 49).

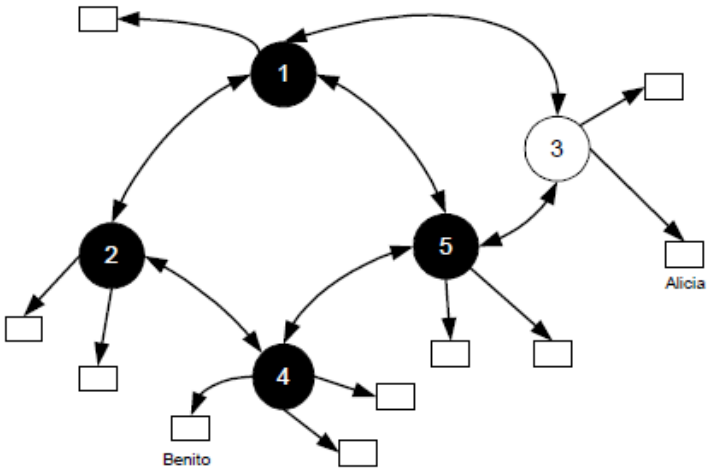


Figura 8. Arquitecturas PKI- Infraestructura en malla

Fuente: (Martínez, 2005)

2.2.11.3 Puente:

La arquitectura de puente fue diseñada para conectar diversas PKIs sin importar su arquitectura. Esto es realizado mediante la introducción de una nueva AC, llamada AC puente, la cual tiene el ´único propósito de establecer relaciones entre las diversas PKIs. A diferencia de las otras arquitecturas, la AC puente no expide certificados directamente a entidades finales. La idea básica es que todos los usuarios PKI consideren la AC puente como un intermediario el cual es capaz de establecer relaciones uno-a-uno con las diferentes PKIs. Estas relaciones pueden ser combinadas para formar un puente de confianza que permita conectar los usuarios de las distintas PKIs.

Si el dominio de confianza es implementado como una PKI jerárquica, la AC puente establece una relación con la AC raíz. Si el dominio es implementado como una PKI de malla, la AC puente establece una relación con solo una de las ACs. En este caso, la AC que establece confianza con la AC puente se denomina AC principal.

2.2.12 Estructuras de datos PKI

Las estructuras de datos básicas utilizadas en PKI son los certificados de llave pública y la lista de revocación de certificados (Martínez, 2005, pág. 50).

2.2.12.1 Certificados X.509

El certificado de llave pública en PKI es definido de acuerdo al estándar X.509. El certificado X.509 ha evolucionado para ser más flexible y poderoso y puede ser usado para portar una gran variedad de información, mucha de la cual es opcional. El certificado de llave pública X.509 está protegido por la firma digital del emisor. Los usuarios del certificado saben que el contenido no ha sido corrompido mediante la verificación del mismo. Los certificados contienen un conjunto de campos comunes, y también pueden incluir opcionalmente una variedad de extensiones. Existen diez campos comunes, seis de los cuales son obligatorios y cuatro opcionales. Los campos obligatorios son: número serial, identificador de algoritmo de la firma, nombre del emisor del certificado, periodo de validez, llave pública, y el nombre del sujeto. Los cuatro campos opcionales son: número de versión, identificadores únicos tanto de emisor como sujeto, y las extensiones. Los campos opcionales aparecen únicamente en los certificados X.509 v2 y X.509 v3.

A continuación se explica a detalle la función de cada campo de un certificado digital X.509 (Martínez, 2005, pág. 51).

Versión. El campo de versión describe la sintaxis del certificado. Existen tres tipos de versiones de certificados. Cuando el campo de versión es omitido, el certificado está codificado en la versión 1. La versión 1 no incluye identificadores ni extensiones.

La versión 2 incluye identificadores pero no extensiones. En la versión 3 se incluyen las extensiones y es la versión más utilizada hoy en día.

Número serial. El número serial es un número entero asignado por el emisor del certificado (la AC). Este número debe de ser único para cada certificado generado. La combinación del número serial y el nombre del emisor identifican únicamente a cualquier certificado.

Firma. El campo de firma indica cual fue el algoritmo de firma digital que fue utilizado para proteger el certificado. Un ejemplo son los tipos de firma utilizados sha256RSA y sha256. La primera parte identifica al criptosistema de llave pública utilizado mientras que la segunda parte identifica al algoritmo hash usado para proteger la integridad del certificado.

Emisor. Este campo contiene el nombre de la entidad que expidió el certificado digital. Este nombre es proporcionado de acuerdo al estándar X.5006.

Validez. El campo de validez indica la fecha en la cual el certificado llega a ser válido y la fecha en la cual el certificado expira.

Sujeto. El campo del sujeto contiene el nombre que identifica al propietario de la llave privada que corresponde a la llave pública que se encuentra en el certificado. El sujeto puede ser cualquier entidad (usuario final, dispositivos de hardware, compañías, etc.).

Información de llave pública. Este campo contiene la llave pública del sujeto, parámetros opcionales y el identificador del algoritmo. La llave pública contenida en este campo es utilizada para verificar las firmas digitales del sujeto. Identificador único del emisor y del sujeto. Estos campos contienen identificadores, y aparecen ´únicamente en las versiones 2 ´o 3. Los identificadores del sujeto y del emisor son utilizados para la reutilización del nombre del emisor y el nombre del sujeto. Sin embargo, se ha probado que este mecanismo no es una solución satisfactoria. Actualmente el RFC3280 no recomienda el uso de estos campos (Martínez, 2005, pág. 52).

Extensiones. Este es un campo opcional y solo aparece en los certificados X.509 versión 3. Si el campo está presente, entonces el certificado contiene una o más extensiones de certificado; cada extensión incluye un identificador de extensión, una bandera que indica si la extensión es crítica o no-crítica, y el valor de la extensión. Comúnmente las extensiones de los certificados han sido definidas por el ISO 7 y ANS I8 y la razón de su existencia es proporcionar mayor flexibilidad del certificado digital. Cualquier organización puede definir una extensión privada para poder cumplir sus requerimientos específicos. Esta flexibilidad crea un nuevo inconveniente: un certificado digital X.509 v3 puede no ser completamente leíble por las implementaciones que soportan certificados X.509 v3. Cuando alguna extensión de certificado no es conocida por la aplicación que lo recibe, la incompatibilidad se hace presente. Esta es la razón por la cual existe la bandera que indica si una extensión es crítica o no crítica. Si la extensión es marcada como no-crítica la aplicación lo ´único que hace es ignorar esa extensión; por otro lado, si es marcada

como crítica el resultado es que el certificado no puede ser utilizado debido a que se desconoce la funcionabilidad de la extension10 .

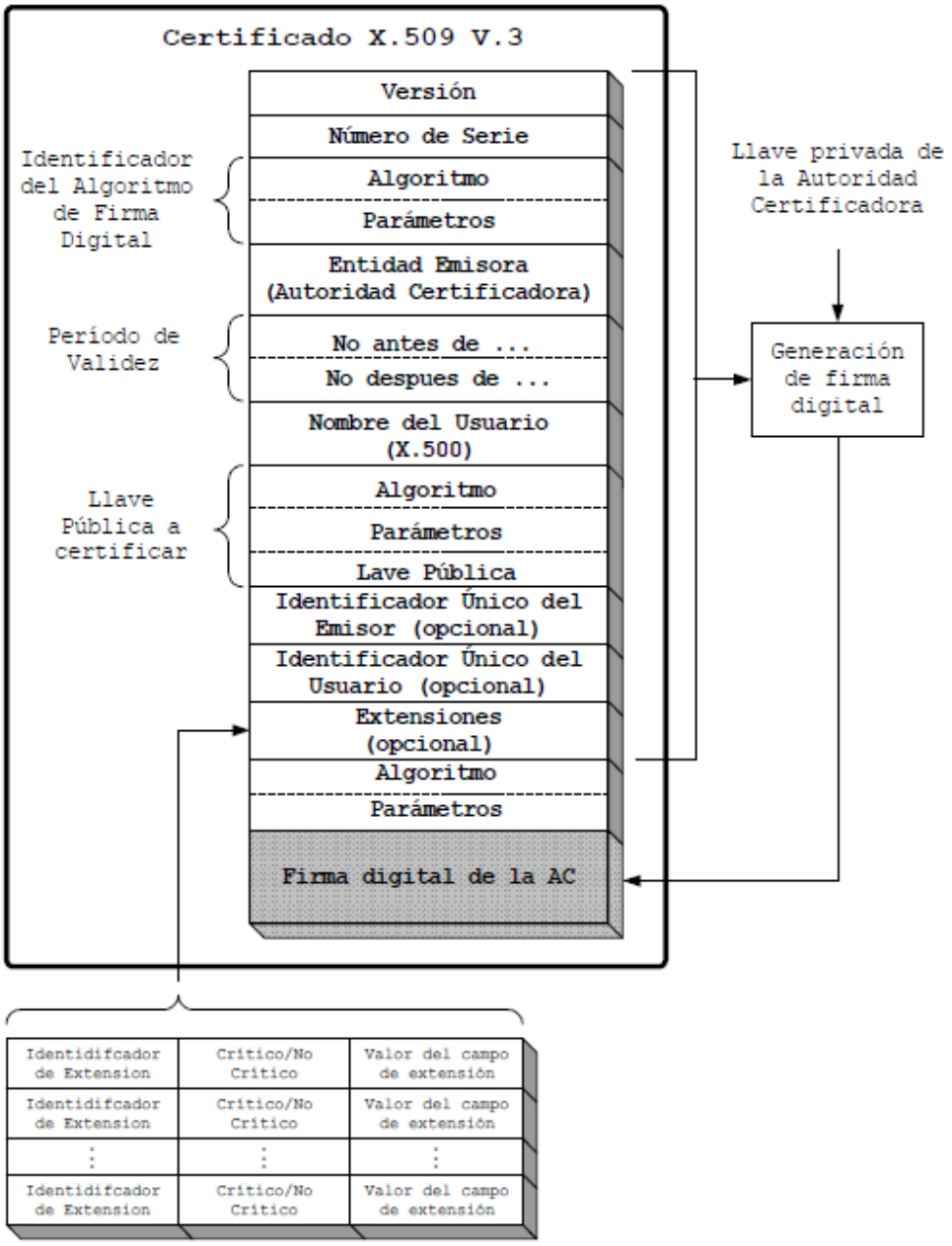


Figura 9. Certificado Digital X.509 versión 3

Fuente: (Martínez, 2005)

2.2.12.2 Listas de revocación de certificados

Los certificados digitales tienen una fecha de expiración establecida. Desafortunadamente, los datos en un certificado digital pueden dejar de ser confiables antes del vencimiento del certificado. Por ejemplo, si una entidad final

cambia la dirección de internet de su compañía la cual está especificada en el certificado digital; o si la llave privada de una usuario fue comprometida. Debido a estas causas, los emisores de certificados necesitan un mecanismo para proporcionar un estado actualizado de los certificados que han emitido. Este mecanismo es denominado X.509 Certification Revocation List (Lista de Revocación de Certificados) X.509.

La CRL está protegida por la firma digital del emisor CRL. Si la firma puede ser verificada, el usuario CRL sabe que el contenido no ha sido corrompido desde que la firma fue generada. Las CRLs contienen varios campos comunes, y al igual que los certificados de llave pública también pueden contener extensiones opcionales.

Los campos que contiene una CRL X.509 son los siguientes:

Versión. Este es un campo opcional y describe la sintaxis de la CRL. La versión más utilizada es la versión 2.

Firma. El campo de firma contiene el identificador del algoritmo utilizado por el emisor CRL para la generación de la firma digital.

Emisor. El campo contiene el nombre X.500 del emisor CRL.

Actualización actual. Este campo indica la fecha de emisión de la CRL.

Actualización siguiente. Este campo indica la fecha de la emisión de la siguiente actualización.

Certificados revocados. El campo contiene una lista de todos los certificados revocados.

Por cada certificado revocado se encuentra una entrada que indica el número serial del certificado revocado, la fecha de revocación, y las entradas de extensiones opcionales CRL. Las entradas de extensiones son empleadas para proporcionar información sobre la revocación de un certificado específico y solamente aparece en la versión 2 (Martínez, 2005, pág. 55).

Extensiones CRL. Este campo es utilizado para proporcionar información adicional acerca de toda la lista de revocación. Aparece ´únicamente en la versión 2 de las CRLs.

En el gráfico N° 2-5 se muestran los campos de una lista de revocación X.509.

El ITU y ANSI han definido varias extensiones para las CRL X.509. Cada extensión al igual que las extensiones de certificados de llave pública pueden ser marcadas como críticas o no-críticas. La verificación de una CRL falla si se desconoce alguna extensión crítica. Sin embargo, las extensiones no reconocidas que son no-críticas simplemente son ignoradas.

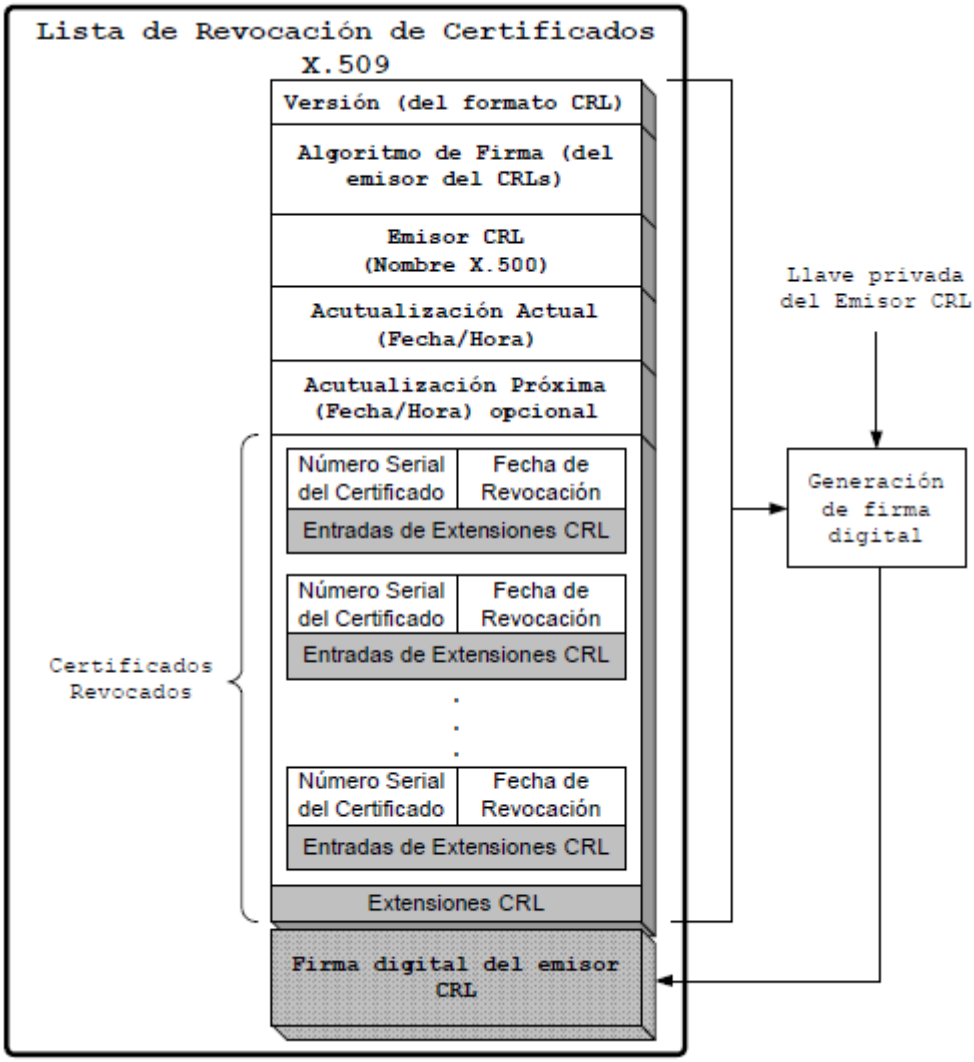


Figura 10. Estructura de una CRL

Fuente: (Martínez, 2005)

CAPÍTULO III

METODOLOGIA DE LA INVESTIGACIÓN

3.1 METODOLOGÍA DE LA INVESTIGACIÓN

La metodología empleada para al análisis técnico del presente estudio toma como referente al documento denominado "Guía de Acreditación de Entidades de Certificación EC Versión 3.3" emitido el año 2007 por el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI, designado como la Autoridad Administrativa Competente (AAC) de Perú en donde se establece los procedimientos y criterios que deben cumplir las Entidades de Certificación, publicación que a su vez está basada en el documento "USA Government Public Key Infrastructure cross certification criteria and methodology"7, vesión 1.3, emitido en Enero del año 2006 por la Autoridad de Políticas de la Infraestructura Federal de PKI del gobierno estadounidense.

Se toma esta referencia "Guía de Acreditación de Entidades de Certificación EC Versión 3.3" debido a que Perú lleva a cabo el proyecto de firma electrónica utilizando el DNI electrónico y en el país no existe una Guía de acreditación para entidades de certificación.

Se realiza en un análisis del Cumplimiento por parte de la DIGERCIC de la Norma ISO 27001:2005 Sistema de Información de Gestión de la Seguridad basada en 11 áreas de control de la norma ISO 27001.

Se realiza un análisis de los requisitos técnicos para Entidades de certificación / Infraestructura de Clave Pública – PKI, Hardware Security Module – HSM, Tarjetas Inteligentes, Certificación, Otros y se realiza una evaluación para verificar el cumplimiento de los requisitos técnicos del sistema magna y la tarjeta de identificación (cedula de identidad).

Se realiza Pruebas de Seguridad en los Sistemas de la DIGERCIC con un test de penetración es decir una evaluación activa de las medidas de seguridad de la información de la DIGERCIC.

Se realiza pruebas de lectura de datos que se encuentran almacenados en el chip que posee la cédula para la evaluación de las seguridades de la tarjeta de identificación (cedula).

3.1.1 Requisitos para Entidades de certificación / Infraestructura de Clave Pública – PKI

Tabla 2.

Entidades de Certificación /Infraestructura de Clave Pública - PKI

Ítem	Referencia	Descripción	Cumple SI/NO
1	X.509 V3	Formatos Estándar para Certificados de Claves Públicas	
2	X.500, X.501, X.509, X.521	Formatos de Nombres para Certificados de Claves Públicas	
3	Estándar Asimétrico RSA	ANSI x3.09 Parte 1	
4	RSA 1024/2048 bits	Soporte para capacidades de longitud de Clave	
5	FIPS 46	Estándar de Cifrado de Datos (DES)	
6	FIPS 180-2	Algoritmo de Hashing SHA-1, SHA-256	
7	FIPS 186	Estándar de Firma Digital (DSA)	
8	Triple DES	CBC Simétrico	
9	FIPS 197	Estándar de Cifrado Avanzado (AES)	
10	CWA 14167 (1-4)	Gestión de Sistemas EC de Confianza	
11	CWA 14169	HSM EAL4+ (Ver conformidad HSM más abajo)	
12	CWA 14172 (1-8)	Directivas CEN para apropiación y operación de EC	
13	CWA 14355	Dispositivos de Creación de Firma Segura	
14	CWA 14365 (1-2)	Uso de las Firmas Electrónicas: Aspectos legales y técnicos	
15	CWA 14890 (1-2)	Interfaz de aplicación para tarjetas inteligentes utilizadas como Dispositivos de Creación de Firma Segura	
16	ETSI SR 002 176	Infraestructuras y Firmas Electrónicas (ESI) – Algoritmos y Parámetros para Firmas Electrónicas Seguras	
17	ETSI TS 101 861	Perfil de Estampa de Tiempo	
18	ETSI TS 102 023	Infraestructuras y Firmas Electrónicas (ESI) – Requisitos de Política para Autoridades de Time-Stamping	
19	ETSI TS 102 040	Infraestructuras y Firmas Electrónicas (ESI) – Armonización Internacional de Requisitos de Política para ECs emisoras de Certificados	
20	ETSI TS 102 042	Requisitos de Política para Entidades de Certificación que emiten Certificados de Clave Pública	

CONTINÚA →

21	ETSI TS 102 280	X.509 V.3 Perfil de Certificado para Certificados emitidos a Personas Naturales
22	IETF RFC 373	Juegos de Caracteres Arbitrarios
23	IETF RFC 1422	Sólo lo relacionado a certificados en general, gestión de claves y Lista de Revocación de Certificados [CRL]
24	IETF RFC 2459	Certificado y Perfil CRL X.509 para PKI
25	IETF RFC 2560	Protocolo OCSP (Protocolo de Estado de Certificado en Línea) X.509 para PKI
26	IETF RFC 3280	Certificado y Perfil CRL X.509 para PKI
27	IETF RFC 3039	Perfil de Certificados Calificados X.509 para PKI
28	IETF RFC 3629	IETF RFC 3629 RFC 3629 - UTF-8, un formato de conversión, formato de la norma ISO 10646
29	IETF RFC 3647	IETF RFC 3647 Sistema básico de Política de Certificados y Prácticas de Certificación X.509 para PKI
30	ISO 27001	Metodología, Transferencia del Conocimiento y Servicio
31	ISO 15408	Tecnología de la Información — Criterios de Evaluación de Técnicas de Seguridad para TI
32	ISO/IEC TR13335	Tecnología de la Información — Guías para la gestión de la Técnicas de Seguridad para TI deben ser implementados y deben ser especificados por una EC.
33	PKCS#1	Estándar de Criptografía RSA: define la criptografía RSA
34	PKCS#3	Estándar de Acuerdo de Clave Diffie-Hellman
35	PKCS#5	PKCS#5 Estándar de Criptografía basada en Contraseña: define cómo cifrar y descifrar datos usando contraseñas
36	PKCS#7	Estándar de Sintaxis de Mensaje Criptográfico: describe una sintaxis general para datos que puedan tener criptografía aplicada en sí mismos, tales como firmas digitales y sobres digitales
37	PKCS#8	Estándar de Sintaxis de Información de Clave Privada: describe una sintaxis para información de clave privada donde ésta incluye una clave privada para algún algoritmo de clave pública y un conjunto de atributos
38	PKCS#9	Clases de Objetos Seleccionados y Tipos de Atributos: define dos nuevas clases de objetos auxiliares, pkcsEntity y naturalPerson, y también tipos de atributos para usarse con estas clases
39	PKCS#10	Estándar de Sintaxis de Solicitud de Certificación: describe la sintaxis para una solicitud de certificación donde ésta consista de un nombre distinguido, una clave pública y, opcionalmente, un conjunto de atributos, firmados colectivamente por la entidad que solicita la certificación**.**
40	PKCS#11	Estándar de Interfaz de Token Criptográfico: especifica una interfaz de programación de aplicación (API), denominada “Cryptoki”, para dispositivos que contengan información criptográfica y realicen funciones criptográficas
41	PKCS#12	Sintaxis de Intercambio de Información Personal: describe una sintaxis de transferencia para información de identidad personal, incluyendo claves privadas, certificados, secretos misceláneos y extensiones.
42	PKCS#15	Se aplica en realidad a proveedores de tarjetas inteligentes
43	RFC 2527	RFC 2527 Lineamientos para Declaración de Prácticas de Certificación [CPS] y Políticas de Certificados [CP]

CONTINÚA →

44	RFC 2587	Diagrama LDAPv2 X.509 para PKI
45	RFC 2818	HTTP sobre TLS
46	IETF RFC 3379	IETF RFC 3379 Requisitos para Validación de Ruta Delegada y para el Protocolo de Descubrimiento de Ruta Delegada
47	TIA - 942	TIA - 942 Estándar de la Infraestructura de Telecomunicaciones para Centros de Datos

Fuente: (INDECOPI, 2007)

3.1.2 Requisitos para Hardware Security Module – HSM[1]

Tabla 3.

Requisitos para Hardware Security Module

Ítem	Referencia	Descripción	Cumple SI/NO
1	Common Criteria	Hardware HSM; el proveedor HSM deberá confirmar su cumplimiento	
2	EAL	Hardware HSM; el proveedor HSM deberá confirmar su cumplimiento	
3	FIPS 140	Requisitos de Seguridad para Módulos Criptográficos: hardware y firmware	

Fuente: (INDECOPI, 2007)

3.1.3 Requisitos para Tarjetas Inteligentes

Tabla 4.

Requisitos para Tarjetas Inteligentes

Ítem	Referencia	Descripción	Cumple SI/NO
1	EAL4+	Requisitos de Seguridad para Módulos Criptográficos: hardware y firmware	
2	Validación FIPS 140-2	Requisitos de Seguridad para Módulos Criptográficos: hardware y firmware	
3	Compatibilidad ISO 7816 1-5	Microcontrolador y Unidad de Procesamiento Numérico (NPU) suplementario capaces de calcular operaciones criptográficas acordes con PKCS #11 y PKCS #15, de conformidad con los requisitos del ISO/IEC 7816-1 al 7816-5	
4	Procesador criptográfico de 32 bits	Para ejecución y usabilidad mejoradas de la tarjeta	
5	Soporte para RSA de 1024/2048 bits	Capacidades de longitud de Clave	
6	Soporte para algoritmo DES	Algoritmo Simétrico	
7	Soporte para algoritmo 3DES	Algoritmo Simétrico	

CONTINÚA

[1] Módulo de Hardware de Seguridad (HSM – Hardware Security Module): dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas

8	Software CSP	Software CSP Proveedor de Servicios Criptográficos [CSP] en el SO del chip capaz de ejecutar funciones criptográficas

Fuente: (INDECOPI, 2007)

Tabla 5.

Requisitos Certificación

Ítem	Referencia	Descripción	Cumple SI/NO
1	FIPS 140-2 Nivel 3[2]	Para HSM, nivel total alcanzado	
2	Certificación EAL4+	Para tarjeta inteligente	
3	Certificación EMC	Para lector de tarjeta inteligente	
4	Certificación ISO 27001	Del entorno	

Fuente: (INDECOPI, 2007)

Tabla 6.

Otros Requisitos

Ítem	Referencia	Descripción	Cumple SI/NO
1	RFC 3161	Protocolo de Sello de Tiempo (TSP) X.509 para PKI	
2	RFC 3628	RFC 3628 Requerimientos de Políticas para Autoridades de Sello de Tiempo (TSAs)	
3	RFC 2246	Protocolo TLS	
4	RFC 2510	Protocolos de Administración de Certificados X.509 para PKI	
5	RFC 2630	Sintaxis para Mensajes Criptográficos	
6	RFC 2634	Optimización de los Servicios de seguridad para S/MIME	
7	RFC 1231	Algoritmo de Hashing MD5	
8	RFC 3126	Formato de firma electrónica para formas electrónicas a largo plazo	

Fuente: (INDECOPI, 2007)

Además se realiza un análisis de Fortalezas, Oportunidades, Debilidades y Amenazas - FODA para la implementación del servicio de firma electrónica por parte de la DIGERCIC.

[2] FIPS (Federal Information Processing Standard) 140 nivel 3: estándar de seguridad de ordenadores del gobierno de los Estados Unidos para la acreditación de módulos criptográficos. En su nivel 3 asegura que los módulos sean resistentes a la intrusión física.

3.1.4 Método de investigación, técnicas e instrumentos de recolección y procesamiento de datos e información.

Para verificar si la infraestructura actual de la DIGERCIC permite la implementación del servicio de firma electrónica se utilizará la metodología descriptiva que permitirá exponer las características de la infraestructura civil, tecnológica, operativa de la Dirección General de Registro Civil Identificación y Cedulación a nivel nacional.

Las principales fuentes de información para el presente trabajo son personal técnico de la DIGERCIC, instrumentos de recolección, material bibliográfico, encuestas, libros, tesis de grado, normas internacionales, leyes y reglamentos vigentes.

Para el procesamiento y la tabulación de la información que se desarrolla en este proyecto de tesis se utilizarán los siguientes programas: Microsoft Office (Word, Excel, Project, Visio).

CAPÍTULO IV

EVALUACIÒN DE LOS REQUISITOS TECNICOS

4.1 ANÁLISIS DEL CUMPLIMIENTO DE LA NORMA ISO 27001:2005 SISTEMA DE INFORMACIÓN DE GESTIÓN DE LA SEGURIDAD

Se ha realizado una encuesta a los responsables de la Dirección de Tecnologías de la DIGERCIC basada en 11 áreas de control de la norma ISO 27001 para medir el nivel de cumplimiento de la norma ISO 27001:2005 Sistema de Información de Gestión de la Seguridad. Ver formato de encuesta anexo A.

Áreas de Control

1. Política de Seguridad
2. Organización de la Seguridad de la Información
3. Gestión de Activos
4. Seguridad en los Recursos Humanos
5. Seguridad física y del entorno
6. Gestión de comunicaciones y operaciones
7. Control de accesos
8. Adquisición, desarrollo y mantenimiento de sistemas de información
9. Gestión de incidentes de seguridad
10. Gestión de continuidad del negocio
11. Cumplimiento

A continuación se presentan los resultados:

4.1.1 A.5 Políticas de Seguridad

La DIGERCIC no cuenta con una política de seguridad de la información aprobada por la Dirección General sin embargo cuenta con procesos y procedimientos establecidos que aseguran parcialmente las políticas de seguridad. Actualmente se están levantando y documentado los procesos para cumplir con este punto.

De acuerdo con la norma una política de seguridad de la información debe ser revisada a intervalos planificados y aprobada por las máximas autoridades lo que actualmente la DIGERCIC no lo ha realizado, este punto afectaría en el momento

que se implemente el nuevo servicio de firma electrónica debido a que la DIGERCIC tendrá que aprobar la política para asegurar su convivencia, adecuación y eficacia con los servicios que han ingresado a producción el último año.

4.1.2 A.6 Aspectos Organizativos de la Seguridad de la Información

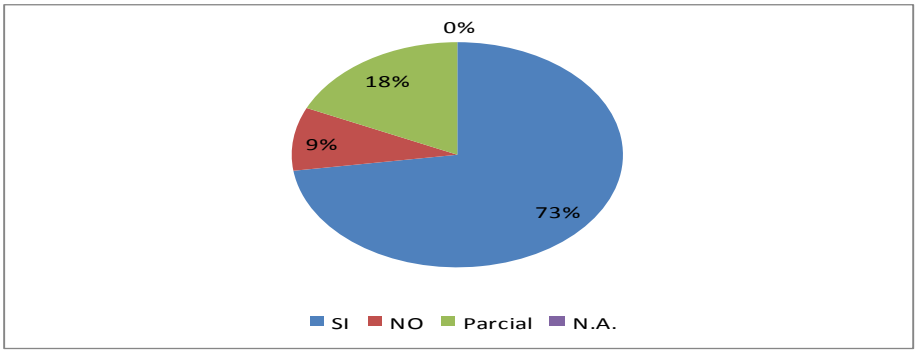


Figura 11. Aspectos Organizativos de la seguridad de la información en la DIGERCIC

La Dirección General aprueba la política de seguridad de la información, asigna los roles de seguridad y coordina y revisa la implementación de la seguridad en toda la organización. Sin embargo es necesario que la DIGERCIC realice una revisión independiente de la seguridad de la información, además los responsables del área de Tecnología deben mantener un contacto activo con grupos de interés especializados en seguridad y realizar una identificación de los riesgos derivados del acceso de terceros.

4.1.3 A.7 Gestión de Activos

Respecto a la gestión de activos la DIGERCIC cumple de forma parcial con el objetivo de conseguir y mantener una protección adecuada de sus activos.

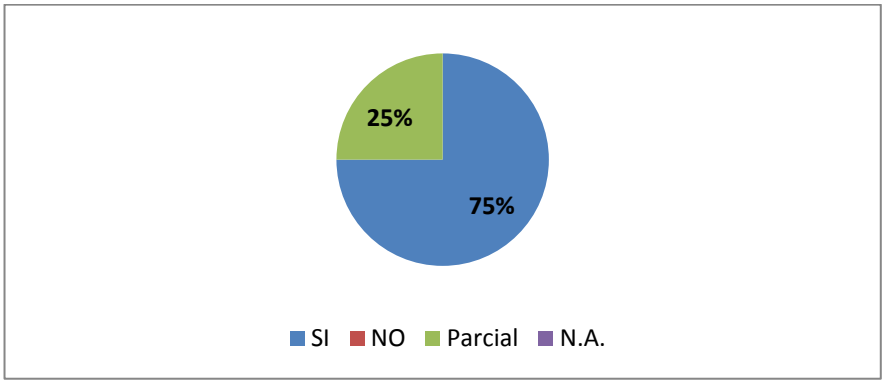


Figura 12. Gestión de Activos

Es en esta área donde la DIGERCIC debe trabajar para que se cumpla con lo establecido en la norma debido a que sus activos son los documentos físicos, actas, archivos biométricos de los ecuatorianos y extranjeros residentes en el Ecuador y se debe conseguir que se mantenga una protección adecuada de los mismos.

La gestión de activos es un área crítica para la implementación del servicio de firma electrónica en razón que esta debe cumplir con el atributo de Integridad, el documento no puede ser alterado de forma alguna durante la transmisión.

4.1.4 A.8 Seguridad en la Contratación de los Recursos Humanos

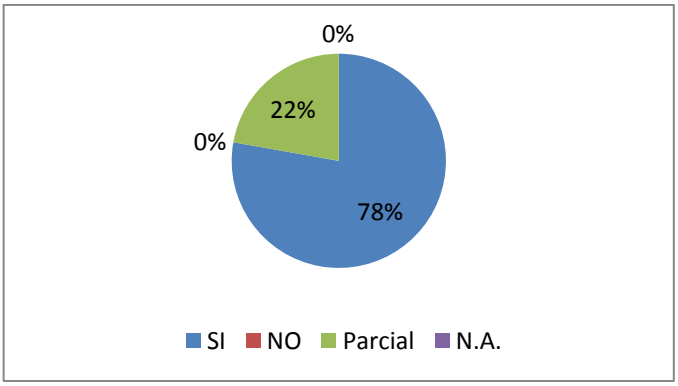


Figura 13. Seguridad en la contratación de los recursos humanos de la DIGERCIC

La DIGERCIC cumple de manera parcial con la seguridad en la contratación de los recursos humanos. En este contexto, los empleados, los contratistas y los terceros antes de su contratación conocen y comprenden sus responsabilidades para llevar a cabo las funciones que les corresponden así como para reducir el riesgo de robo, fraude o de uso indebido de los recursos. Se verifica también que todos los empleados, contratistas y terceros durante su contratación son conscientes de las amenazas y problemas que afectan a la seguridad de la información y de sus responsabilidades y obligaciones, y de que están preparados para cumplir la política de seguridad en el desarrollo habitual de su trabajo, y para reducir el riesgo de error humano. Además se asegura que los empleados, contratistas y terceros abandonan la organización o cambian de puesto de trabajo de una manera ordenada.

Sin embargo la DIGERCIC debe identificar y evaluar los riesgos que implica el acceso a la información de la DIGERCIC de los contratistas o de terceros.

4.1.5 A.9 Seguridad Física y Ambiental

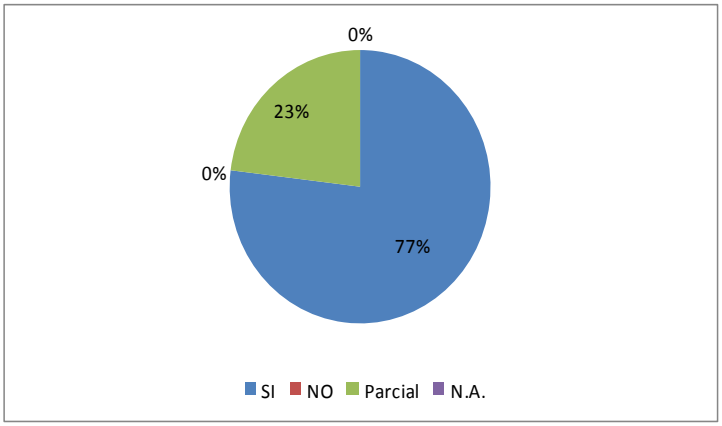


Figura 14. Seguridad Física y Ambiental de la DIGERCIC

En forma parcial se previenen los accesos físicos no autorizados, los daños y las intromisiones en las instalaciones y en la información de la DIGERCIC.

La seguridad física y ambiental se debe reforzar en oficinas, despachos e instalaciones cantonales donde todavía no se ha ejecutado el proyecto de modernización, se debe proteger contra las amenazas externas y de origen ambiental. Y se debe reforzar la seguridad en las áreas de acceso público y de carga y descarga.

4.1.6 A.10 Gestión de Comunicaciones y Operaciones

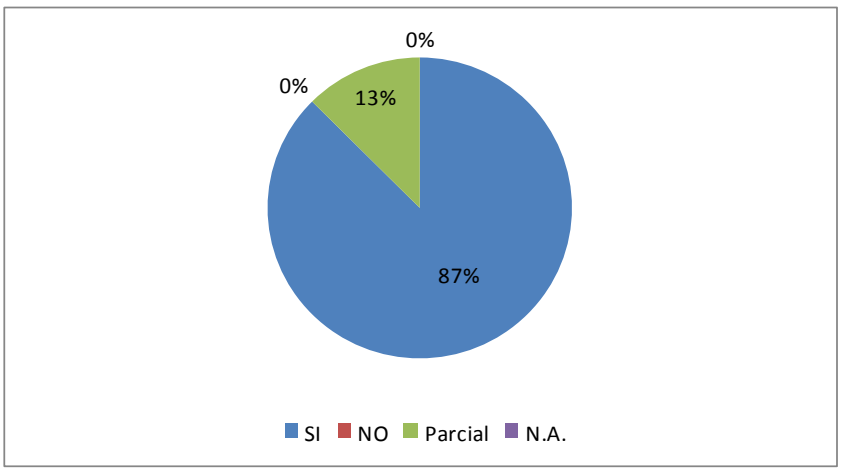


Figura 15. Gestión de Comunicaciones y Operaciones de la DIGERCIC

La DIGERCIC asegura el funcionamiento correcto de los sistemas de identificación Magna, el sistema de identificación biométrica, sistemas de interoperabilidad; implanta y mantiene el nivel apropiado de seguridad de la

información en la provisión del servicios que brinda a la ciudadanía, además de minimizar el riesgo de fallos de los sistemas.

Protege la integridad del software y de la información, mantiene la integridad y disponibilidad de la información y de los recursos de tratamiento de la información. Asegura la protección de la información en las redes y la protección de la infraestructura de soporte.

Evita la revelación, modificación, retirada o destrucción no autorizada de los activos, y la interrupción de las actividades de la organización. Mantiene la seguridad de la información y del software intercambiados dentro de una organización y con un tercero, detecta las actividades de tratamiento de la información no autorizadas.

Sin embargo la DIGERCIC debe implantar y mantener el nivel apropiado de seguridad de la información en la provisión del servicio, en concordancia con los acuerdos de provisión de servicios por terceros. Los servicios, informes y registros proporcionados por un tercero deben ser objeto de supervisión y revisión periódica, y también deben realizar auditorías periódicas así como la reevaluación de los riesgos.

La Gestión de Comunicaciones y Operaciones es un tema prioritario para la implementación del servicio de firma electrónica debido a que la firma electrónica se sustenta en la operación de los sistemas de información.

4.1.7 A.11 Control de Acceso

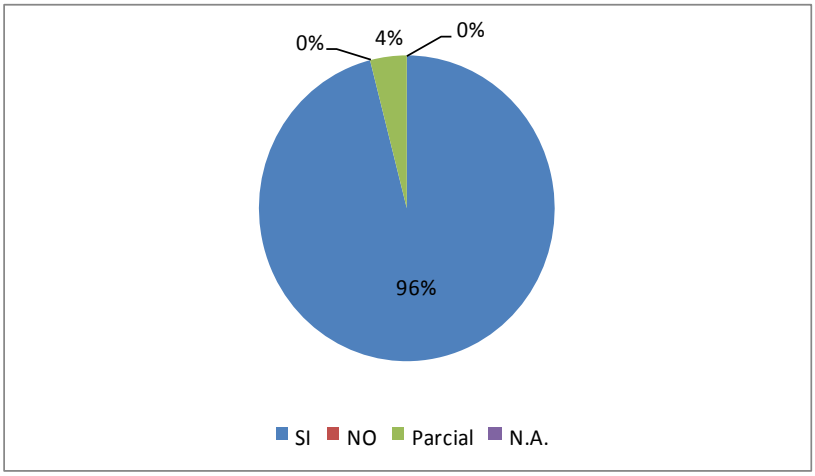


Figura 16. Control de Acceso de la DIGERCIC

La DIGERCIC debido a que maneja información personal de los ecuatorianos mantiene un estricto control al acceso a la información, asegura el acceso de un

usuario autorizado a los sistemas de información, previene el acceso de usuarios no autorizados, así como evita que se comprometa o se produzca el robo de información o de recursos de tratamiento de la información. Previene el acceso no autorizado a: los servicios en red, sistemas operativos, a la información que contienen las aplicaciones. Garantiza la seguridad de la información cuando se utilizan ordenadores portátiles y comunicaciones móviles especialmente en brigadas móviles para la atención en zonas rurales y de la frontera donde no existen oficinas de Registro Civil.

La DIGERCIC para cumplir completamente con la norma debe concientizar a los funcionarios para que adopten una política de puesto de trabajo despejado de papeles y de soportes de almacenamiento extraíbles junto con una política de pantalla limpia para los recursos de tratamiento de la información.

4.1.8 A.12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

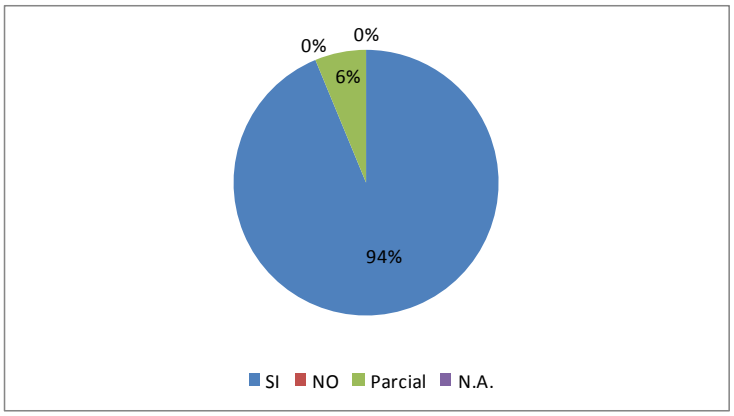


Figura 17. Adquisición, desarrollo y mantenimiento de los sistemas de información de la DIGERCIC

La DIGERCIC cuando adquiere, desarrolla y mantiene los Sistemas de Información garantiza que la seguridad está integrada en los sistemas de información. Evita errores, pérdida, modificaciones no autorizadas o usos indebidos de la información en las aplicaciones. Protege la confidencialidad, la autenticidad o la integridad de la información por medios criptográficos. Garantiza la seguridad de los archivos de sistema, mantiene la seguridad del software y de la información de las aplicaciones

Sin embargo debe reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas para ello debe obtener la información adecuada acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados, debe evaluar la exposición de la organización a dichas vulnerabilidades y debe adoptar las medidas adecuadas para afrontar el riesgo asociado.

4.1.9 A.13 Gestión de Incidentes de Seguridad de la Información

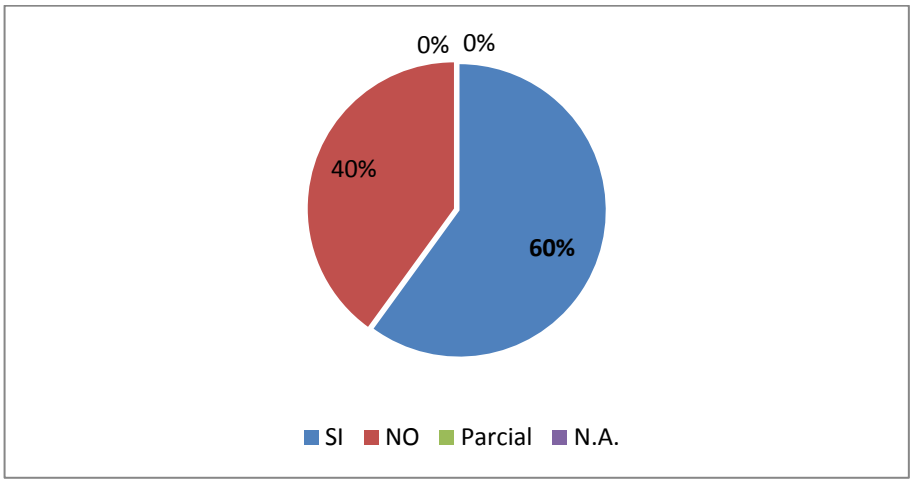


Figura 18. Gestión de incidentes de seguridad de la información de la DIGERCIC

Como puede observarse en la gráfica anterior la gestión de incidentes de seguridad de la información no es adecuada.

La DIGERCIC no garantiza que se aplique un enfoque coherente y efectivo a la gestión de los incidentes de seguridad de la información, para cumplir con el objetivo de la norma en este punto. Se debe establecer mecanismos que permitan cuantificar y supervisar los tipos, volúmenes y coste de los incidentes de seguridad de la información. Además cuando se emprende una acción contra una persona u organización, después de un incidente de seguridad de la información, que implique acciones legales (tanto civiles como penales), se debe garantizar que se logre recopilar las evidencias, y que se conserven y presenten conforme a las normas establecidas en la jurisdicción correspondiente.

4.1.10 A.14 Gestión de la Continuidad del Negocio

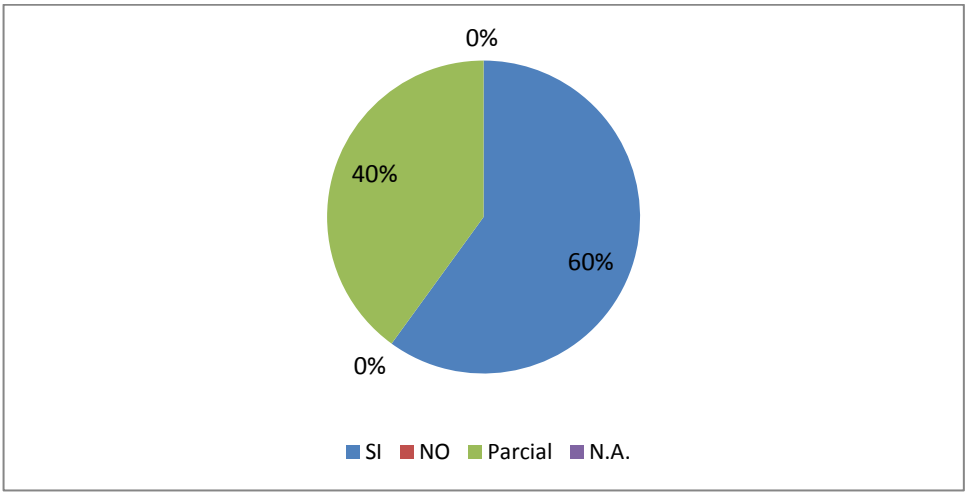


Figura 19. Gestión de la continuidad del negocio de la DIGERCIC

La DIGERCIC en un 60% contrarresta las interrupciones de las actividades empresariales y protege los procesos críticos de negocio de los efectos derivados de fallos importantes o catastróficos de los sistemas de información, así como garantizar su oportuna reanudación.

Lo anterior es debido a que la DIGERCIC respecto a la continuidad del negocio y evaluación de riesgos no identifica los eventos que puedan causar interrupciones en los procesos de negocio, así como la probabilidad que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información.

4.1.11 A 15 Cumplimiento de reglamentación

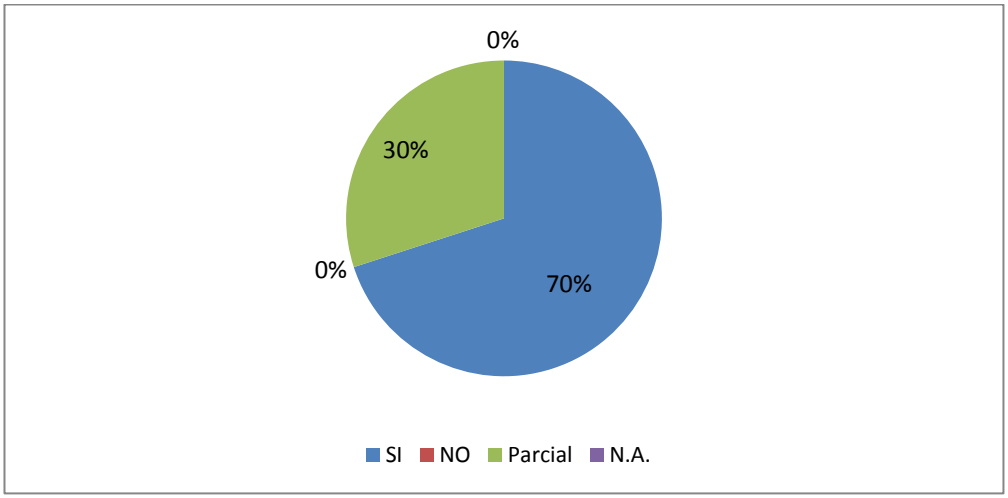


Figura 20. Cumplimiento de reglamentación en la DIGERCIC

En la mayoría de casos la DIGERCIC no sigue estrictamente la reglamentación de requisitos de seguridad.

Con respecto a la protección de los documentos de la organización existen documentos importantes tales como los archivos provinciales, cantonales y parroquiales que no están protegidos contra la perdida, destrucción y falsificación en especial de las agencias que no se han modernizado.

También se debe indicar que el área de Tecnología no comprueba periódicamente que los sistemas de información cumplen las normas de aplicación para la implantación de la seguridad.

4.2 PRUEBAS DE SEGURIDAD EN LOS SISTEMAS DE LA DIGERCIC

Se realizó un test de penetración es decir una evaluación activa de las medidas de seguridad de la información de la DIGERCIC.

Las pruebas de penetración nos permiten conocer el nivel de seguridad externa de los sistemas de información de la DIGERCIC, determinando el grado de acceso que tendría un atacante con intenciones maliciosas.

4.2.1 Pruebas Externas

Fase 1 Reconocimiento

En esta etapa se obtuvo la información de los sistemas web y de correo electrónico de la DIGERCIC como: direcciones IP, nombres de servidores, nombres de usuario potenciales que aparecen en la lista como contactos con la ayuda de las herramientas nslookup, whois de LACNIC.

Información servidor web

Nombre de dominio: www.registrocivil.gob.ec

Dirección IP: 200.107.60.56

Rango IP: 200.107.32.0 - 200.107.63.255

Información servidor de correo

Nombre de dominio: mailserver.registrocivil.gob.ec

Dirección IP: 190.152.146.147

https://mailserver.registrocivil.gob.ec/zimbra/

Rango IP: 190.152.128.0 - 190.152.255.255

Fase 2. Exploración.

En la fase de exploración se realizó un traceroute, escaneo de puertos y vulnerabilidades de los servidores web y de correo electrónico de donde se obtuvo los siguientes resultados:

Traceroute www.registrocivil.gob.ec:

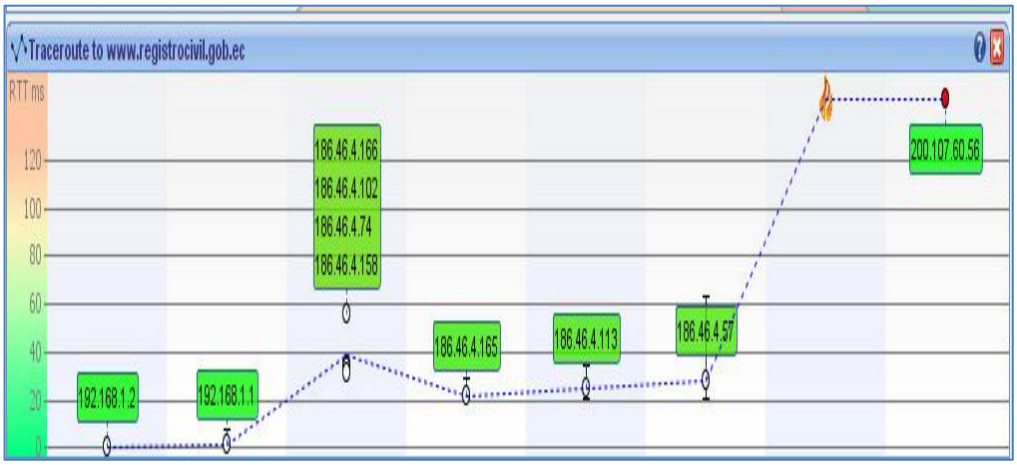


Figura 21. Traceroute www.registrocivil.gob.ec

Traceroute mailserver.registrocivil.gob.ec:

Figura 22. Traceroute mailserver.registrocivil.gob.ec

Para realizar el traceroute se utilizó la herramienta VisualRoute 2010, para el escaneo de puertos NetScanTools, y Nessus para el escaneo de vulnerabilidades.

Escaneo de puertos del Servidor Web

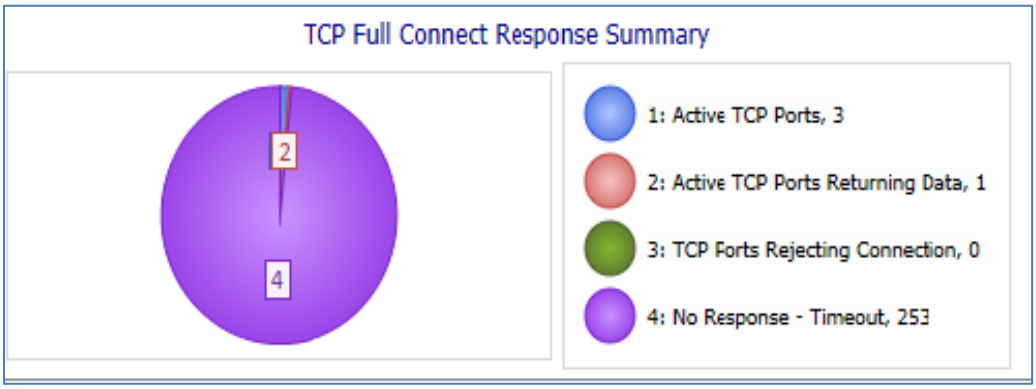


Figura 23. Resultado Escaneo puertos TCP

Tabla 7.

Lista de puertos abiertos servidor web

IP Address	Puerto	Puerto Descripción	Protocolo	Resultado	Dato recibido
200.107.60.56	21	ftp	TCP	Port Active	220 ProFTPD 1.3.4a Server (ProFTPD server) [::ffff:200.107.60.56]
200.107.60.56	80	http	TCP	Port Active	
200.107.60.56	81	hosts2-ns	TCP	Port Active	

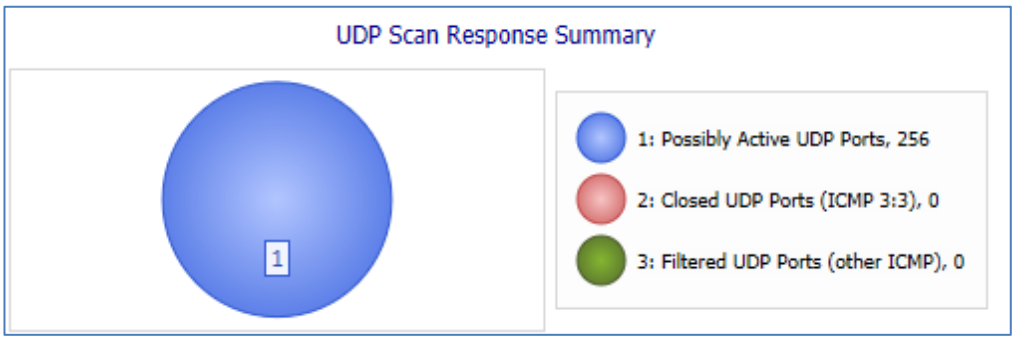


Figura 24. Resultado Escaneo puertos UDP

Vulnerabilidades servidor web: 200.107.60.56

Cuadro 1.

Vulnerabilidades Servidor Web

Critical	High	Medium	Low	Info	Total
0	0	0	1	25	26

El servidor web presenta solo una vulnerabilidad de bajo factor de riesgo que se describe a continuación.

21/tcp: 34324 - FTP Supports Clear Text Authentication

Sinopsis

Las credenciales de autenticación pueden ser interceptadas.

Descripción

El servidor FTP remoto permite que el nombre y la contraseña que se transmite en texto plano del usuario, que puede ser interceptada por un sniffer de red o un ataque man-in-the middle.

Solución

Cambiar a SFTP (parte de la suite SSH) o FTPS (FTP sobre SSL / TLS). En este último caso, configurar el servidor de modo que las conexiones de control sean encriptadas.

Vulnerabilidades servidor de correo: 190.152.146.147

Cuadro 2.

Vulnerabilidades Servidor Correo

Critical	High	Medium	Low	Info	Total
0	0	0	2	34	36

El servidor de correo presenta dos vulnerabilidades de bajo factor de riesgo que se describe a continuación.

1. 80/tcp 10759 - Web Server HTTP Header Internal IP Disclosure

Sinopsis

El servidor web permite fugas de una dirección IP privada a través de las cabeceras HTTP.

Descripción

Esto puede exponer a las direcciones IP internas que están generalmente ocultos o enmascarados detrás de una traducción de direcciones de Servidor de seguridad de red (NAT) o un servidor proxy.

Hay un problema conocido con Microsoft IIS 4.0 haciendo esto en su configuración por defecto. Esto también puede afectar otros servidores web,

aplicaciones web, servidores proxy web, balanceadores de carga ya través de una variedad de configuraciones erróneas relacionadas con el cambio de dirección.

Solución: Ninguno

110/tcp 143/tcp 443/tcp 65821 - SSL RC4 Cipher Suites Supported

Sinopsis

El servicio remoto admite el uso del sistema de cifrado RC4.

Descripción

El host remoto admite el uso de RC4 en uno o más conjuntos de cifrado. El sistema de cifrado RC4 es defectuoso en su generación de una secuencia pseudo-aleatoria de bytes de modo que una amplia variedad de pequeños sesgos se introducen en la trama, disminuyendo su aleatoriedad.

Si es texto plano repetidamente cifrado (por ejemplo, cookies HTTP), y un atacante puede obtener muchos (es decir, decenas de millones) textos cifrados, el atacante puede ser capaz de obtener el texto en claro.

Solución

Vuelva a configurar la aplicación afectada, si es posible, evitar el uso de algoritmos de cifrado RC4.

4.2.2 Pruebas Internas

Escaneo de puertos del Servidor Magna

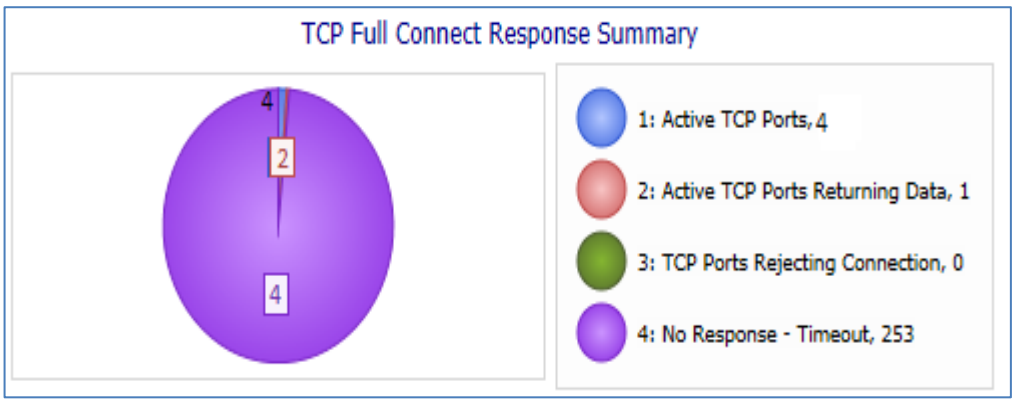


Figura 25. Resultado Escaneo puertos UDP

Tabla 8.

Lista de puertos abiertos servidor

IP Address	Puerto	Puerto Descripción	Protocolo	Resultado	Dato recibido
10.20.20.4	21	ftp	TCP	Port Active	220 ProFTPD 1.3.4a Server (ProFTPD server) [::ffff:200.107.60.56]
10.20.20.4	80	http	TCP	Port Active	
10.20.20.4	81	hosts2-ns	TCP	Port Active	
10.20.20.4	443	Secure Sockets Layer (SSL o "HTTPS")	TCP	Port Active	
10.20.20.4	1723	PPTP	TCP	Port Active	

Vulnerabilidades servidor magna: 10.20.20.4

Cuadro 3.

Vulnerabilidades Servidor Magna

Critical	High	Medium	Low	Info	Total
0	**0**	**0**	**1**	**32**	**33**

El servidor presenta solo una vulnerabilidad de bajo factor de riesgo que se describe a continuación.

21/tcp: 34324 - FTP Supports Clear Text Authentication

Sinopsis

Las credenciales de autenticación pueden ser interceptadas.

Descripción

El servidor FTP remoto permite que el nombre y la contraseña que se transmite en texto plano del usuario, que puede ser interceptada por un sniffer de red o un ataque man-in-the middle.

Solución

Cambiar a SFTP (parte de la suite SSH) o FTPS (FTP sobre SSL / TLS). En este último caso, configurar el servidor de modo que las conexiones de control sean encriptadas.

4.3 PRUEBAS DE LECTURA Y SEGURIDADES DE LA TARJETA DE IDENTIFICACIÓN

Para la evaluación de las seguridades de la tarjeta de identificación se han realizado varias pruebas de lectura de datos que se encuentran almacenados en el chip que posee la cédula.

En ese sentido la lectura de datos de la cédula funcionaba en base a aplicaciones de escritorio basadas en PC como la de la gráfica siguiente; en este tipo de aplicaciones para poder acceder a la información RFID era preciso introducir primero el número de cédula y luego poder proceder con la lectura RFID.

Este tipo de soluciones obedece al siguiente esquema, la comunicación entre los lectores y el computador es serial USB:

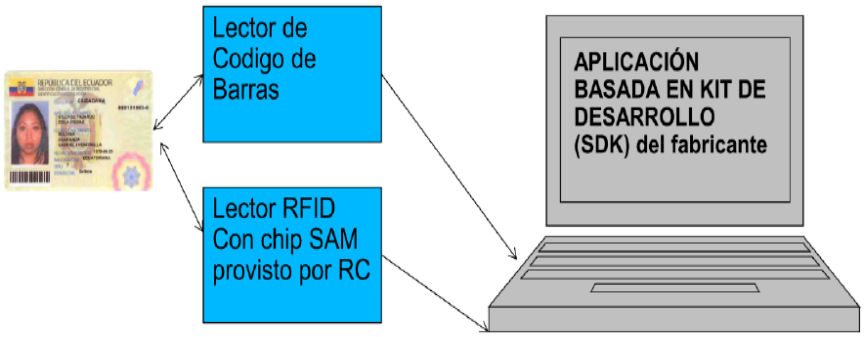


Figura 26. Esquema Lectura datos de la cédula

Fuente: (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2011)

Se efectúa pruebas exitosas de lectura de parámetros encriptados de la cédula de ciudadanía mediante el uso de una herramienta personalizada de prueba para desarrollo de software (Software Development Kit o SDK) y un chip Secured Access Module (SAM) suministrado por el RC.

El SDK, al ser de prueba, solo permite leer algunos textos más no la huella digital o foto; para lo cual se requiere el desarrollo de un SDK que provea la línea completa de comandos para poder acceder, según sea requerido, a cualquier información contenida en la cédula.

Dado que el número de cédula de ciudadanía es una de las claves para poder descifrar el contenido del chip interno; se hace necesario introducirlo, o bien manualmente o bien leyendo el código de barras.

Los datos que contiene el chip de la cédula de ciudadanía se encuentran encriptados por seguridad conforme a normas ICAO 9303 y solo con autorización del Registro Civil pueden ser leídos.

Por lo anteriormente mencionado para poder acceder a información de la cédula, tales como nombre, datos filiatorios, número de cédula, huella, foto, firma, se requiere que el lector RFID cuente con una tarjeta y/o chip SAM (Secured Application Module) para desencriptar la información disponible en la cédula.

El kit de desarrollo de software SDK cumple con la estructura lógica de datos de ICAO (ICAO LDS), con las normas de verificación así como con los estándares biométricos ISO/IEC (Organización Internacional de Normalización/Comisión Electrotécnica Internacional); y se trata de un API (Interfaz de Programación de Aplicaciones) flexible y un juego de herramientas diseñado para leer, escribir, validar y ver los datos del chip de la cédula, proporciona un apoyo integral para los protocolos de seguridad: Control de Acceso Básico (Basic Access Control).

El Control de Acceso Básico (BAC) se utiliza con el fin de prevenir la intercepción y captura de las [PKI] (Infraestructura de Clave Pública). Los mecanismos de control permiten que los datos almacenados en el chip sean leídos de manera segura.

El siguiente Set de comando BAC han sido utilizados en la lectura de información de la cédula electrónica:

- SELECT
- READ BINARY
- UPDATE BINARY
- GET CHALLENGE
- EXTERNAL AUTHENTICATE
- MUTUAL AUTHENTICATE
- CREATE FILE
- DELETE FILE
- PUT DATA
- CHANGE REFERENCE DATA
- VERIFY
- WRITE KEY

Para que los lectores RFID puedan leer y extraer cualquier información de la cédula de identidad, se debe desarrollar una interfaz de comunicación segura entre lector, cédula y aplicaciones.

Para desarrollar la interfaz se requiere de un chip SAM, el cual se utiliza para la autenticación criptográfica entre la cédula y el lector y de un kit de desarrollo de software (SDK), que permitirá integrar con las aplicaciones de que se desee dar a la cédula.

4.4 EVALUACIÓN DE REQUISITOS PARA ENTIDADES DE CERTIFICACIÓN / INFRAESTRUCTURA DE CLAVE PÚBLICA – PKI

En este punto se realiza la evaluación del cumplimiento de los requisitos técnicos del Sistema Magna y de la DIGERCIC para entidades de certificación de acuerdo con la "Guía de Acreditación de Entidades de Certificación EC Versión 3.3". El objetivo es determinar si el sistema Magna y la DIGERCIC están en capacidad técnica de soportar el servicio de firma electrónica.

Tabla 9.

Cumplimiento Requisitos para Entidades de certificación / Infraestructura de Clave Pública – PKI

Ítem	Referencia	Descripción	Cumple SI/NO
1	X.509 V3	Formatos Estándar para Certificados de Claves Públicas	SI
2	X.500, X.501, X.509, X.521	Formatos de Nombres para Certificados de Claves Públicas	SI
3	Estándar Asimétrico RSA	ANSI x3.09 Parte 1	SI
4	RSA 1024/2048 bits	Soporte para capacidades de longitud de Clave	SI
5	FIPS 46	Estándar de Cifrado de Datos (DES)	SI
6	FIPS 180-2	Algoritmo de Hashing SHA-1, SHA-256	SI
7	FIPS 186	Estándar de Firma Digital (DSA)	SI
8	Triple DES	CBC Simétrico	SI
9	FIPS 197	Estándar de Cifrado Avanzado (AES)	SI
10	CWA 14167 (1-4)	Gestión de Sistemas EC de Confianza	SI

CONTINÚA

11	CWA 14169	HSM EAL4+ (Ver conformidad HSM más abajo)	SI
12	CWA 14172 (1-8)	Directivas CEN para apropiación y operación de EC	NO
13	CWA 14355	Dispositivos de Creación de Firma Segura	SI
14	CWA 14365 (1-2)	Uso de las Firmas Electrónicas: Aspectos legales y técnicos	SI
15	CWA 14890 (1-2)	Interfaz de aplicación para tarjetas inteligentes utilizadas como Dispositivos de Creación de Firma Segura	SI
16	ETSI SR 002 176	Infraestructuras y Firmas Electrónicas (ESI) – Algoritmos y Parámetros para Firmas Electrónicas Seguras	SI
17	ETSI TS 101 861	Perfil de Estampa de Tiempo	NO
18	ETSI TS 102 023	Infraestructuras y Firmas Electrónicas (ESI) – Requisitos de Política para Autoridades de Time-Stamping	N O
19	ETSI TS 102 040	Infraestructuras y Firmas Electrónicas (ESI) – Armonización Internacional de Requisitos de Política para ECs emisoras de Certificados	SI
20	ETSI TS 102 042	Requisitos de Política para Entidades de Certificación que emiten Certificados de Clave Pública	NO
21	ETSI TS 102 280	X.509 V.3 Perfil de Certificado para Certificados emitidos a Personas Naturales	SI
22	IETF RFC 373	Juegos de Caracteres Arbitrarios	SI
23	IETF RFC 1422	Sólo lo relacionado a certificados en general, gestión de claves y Lista de Revocación de Certificados [CRL]	SI
24	IETF RFC 2459	Certificado y Perfil CRL X.509 para PKI	SI
25	IETF RFC 2560	Protocolo OCSP (Protocolo de Estado de Certificado en Línea) X.509 para PKI	SI
26	IETF RFC 3280	Certificado y Perfil CRL X.509 para PKI	SI
27	IETF RFC 3039	Perfil de Certificados Calificados X.509 para PKI	SI
28	IETF RFC 3629	IETF RFC 3629 RFC 3629 - UTF-8, un formato de conversión, formato de la norma ISO 10646	SI
29	IETF RFC 3647	IETF RFC 3647 Sistema básico de Política de Certificados y Prácticas de Certificación X.509 para PKI	NO
30	ISO 27001	Metodología, Transferencia del Conocimiento y Servicio	NO
31	ISO 15408	Tecnología de la Información — Criterios de Evaluación de Técnicas de Seguridad para TI	NO
32	ISO/IEC TR13335	Tecnología de la Información — Guías para la gestión de la Técnicas de Seguridad para TI deben ser implementados y deben ser especificados por una EC.	NO
33	PKCS#1	Estándar de Criptografía RSA: define la criptografía RSA	SI
34	PKCS#3	Estándar de Acuerdo de Clave Diffie-Hellman	SI
35	PKCS#5	PKCS#5 Estándar de Criptografía basada en Contraseña: define cómo cifrar y descifrar datos usando contraseñas	SI
36	PKCS#7	Estándar de Sintaxis de Mensaje Criptográfico: describe una sintaxis general para datos que puedan tener criptografía aplicada en sí mismos, tales como firmas digitales y sobres digitales.	SI

CONTINÚA →

37	PKCS#8	Estándar de Sintaxis de Información de Clave Privada: describe una sintaxis para información de clave privada donde ésta incluye una clave privada para algún algoritmo de clave pública y un conjunto de atributos	SI
38	PKCS#9	Clases de Objetos Seleccionados y Tipos de Atributos: define dos nuevas clases de objetos auxiliares, pkcsEntity y naturalPerson, y también tipos de atributos para usarse con estas clases.	SI
39	PKCS#10	Estándar de Sintaxis de Solicitud de Certificación: describe la sintaxis para una solicitud de certificación donde ésta consista de un nombre distinguido, una clave pública y, opcionalmente, un conjunto de atributos, firmados colectivamente por la entidad que solicita la certificación.	SI
40	PKCS#11	Estándar de Interfaz de Token Criptográfico: especifica una interfaz de programación de aplicación (API), denominada "Cryptoki", para dispositivos que contengan información criptográfica y realicen funciones criptográficas	SI
41	PKCS#12	Sintaxis de Intercambio de Información Personal: describe una sintaxis de transferencia para información de identidad personal, incluyendo claves privadas, certificados, secretos misceláneos y extensiones.	SI
42	PKCS#15	Se aplica en realidad a proveedores de tarjetas inteligentes	SI
43	RFC 2527	RFC 2527 Lineamientos para Declaración de Prácticas de Certificación [CPS] y Políticas de Certificados [CP]	NO
44	RFC 2587	Diagrama LDAPv2 X.509 para PKI	SI
45	RFC 2818	HTTP sobre TLS	SI
46	IETF RFC 3379	IETF RFC 3379 Requisitos para Validación de Ruta Delegada y para el Protocolo de Descubrimiento de Ruta Delegada	NO
47	TIA - 942	TIA - 942 Estándar de la Infraestructura de Telecomunicaciones para Centros de Datos	SI

Los ítems 12, 20, 29, 43, 46 no son relevantes su cumplimiento debido a que la DIGERCIC actualmente no es una AC.

Los Ítems 17 y 18 no son relevante su cumplimiento debido a que la DIGERCIC actualmente no es una Autoridad de Sellado de Tiempo - TSA.

Los ítems 31 y 32 son muy relevantes para la implementación del servicio de firma electrónica.

4.4.1 Requisitos para Hardware Security Module – HSM

Tabla 10.

Cumplimiento Requisitos para Hardware Security Module – HSM

Ítem	Referencia	Descripción	Cumple SI/NO
1	Common Criteria	Hardware HSM; el proveedor HSM deberá confirmar su cumplimiento	SI
2	EAL	Hardware HSM; el proveedor HSM deberá confirmar su cumplimiento	SI
3	FIPS 140	Requisitos de Seguridad para Módulos Criptográficos: hardware y firmware	SI

4.4.2 Requisitos para Tarjetas Inteligentes

Tabla 11.

Cumplimiento Requisitos para Tarjetas Inteligentes

Ítem	Referencia	Descripción	Cumple SI/NO
1	EAL4+	Requisitos de Seguridad para Módulos Criptográficos: hardware y firmware	SI
2	Validación FIPS 140-2	Requisitos de Seguridad para Módulos Criptográficos: hardware y firmware	SI
3	Compatibilidad ISO 7816 1-5	Microcontrolador y Unidad de Procesamiento Numérico (NPU) suplementario capaces de calcular operaciones criptográficas acordes con PKCS #11 y PKCS #15, de conformidad con los requisitos del ISO/IEC 7816-1 al 7816-5	SI
4	Procesador criptográfico de 32 bits	Para ejecución y usabilidad mejoradas de la tarjeta	SI
5	Soporte para RSA de 1024/2048 bits	Capacidades de longitud de Clave	SI
6	Soporte para algoritmo DES	Algoritmo Simétrico	SI
7	Soporte para algoritmo 3DES	Algoritmo Simétrico	SI
8	Software CSP	Software CSP Proveedor de Servicios Criptográficos [CSP] en el SO del chip capaz de ejecutar funciones criptográficas	SI

Tabla 12.

Cumplimiento Requisitos para Certificación

Ítem	Referencia	Descripción	Cumple SI/NO
1	FIPS 140-2 Nivel 3	Para HSM, nivel total alcanzado	SI
2	Certificación EAL4+	Para tarjeta inteligente	SI
3	Certificación EMC	Para lector de tarjeta inteligente	SI
4	Certificación ISO 27001	Del entorno	NO

Tabla 13.

Cumplimiento Otros Requisitos

Ítem	Referencia	Descripción	Cumple SI/NO
1	RFC 3161	Protocolo de Sello de Tiempo (TSP) X.509 para PKI	NO
2	RFC 3628	RFC 3628 Requerimientos de Políticas para Autoridades de Sello de Tiempo (TSAs)	NO
3	RFC 2246	Protocolo TLS	SI
4	RFC 2510	Protocolos de Administración de Certificados X.509 para PKI	SI
5	RFC 2630	Sintaxis para Mensajes Criptográficos	SI
6	RFC 2634	Optimización de los Servicios de seguridad para S/MIME	NO
7	RFC 1231	Algoritmo de Hashing MD5	SI
8	RFC 3126	Formato de firma electrónica para formas electrónicas a largo plazo	SI

Por otra parte del análisis de los requisitos para que la DIGERCIC sea una entidad certificadora conforme la resolución RES 477-20-CONATEL-2008-Modelo de Acreditación como entidad de certificación de información y servicios relacionados.

De acuerdo con el Art 3- Responsabilidades, punto 1, la DIGERCIC no cuenta con una declaración de Prácticas de Certificación, en el capítulo IV se

presentan recomendaciones para el desarrollo de una declaración de Prácticas de Certificación.

Para el punto 2 (Art 3) la DIGERCIC no cuenta con una declaración de Políticas de Seguridad aprobada, sin embargo se están levantando los procedimientos y normas de seguridad, esta política debe revisarse y adaptarse a las condiciones y procedimientos relativos a la seguridad de la infraestructura de una Entidad de Certificación de Información y seguridad en la prestación de servicios de certificación de información y servicios relacionados con la firma electrónica.

Para el punto 2. Contar con una declaración de Políticas de Seguridad, numeral a) la DIGERCIC en la Dirección de Gestión Tecnológica cuenta con un grupo de personal técnico que está a cargo de llevar a cabo los procedimientos de seguridad para el manejo de eventos de seguridad en los sistemas de identificación (Magna, AS400), AFIS, bases de datos, equipos de red, y más.

4.5 EVALUACIÓN DE LAS SEGURIDADES DE LA INFORMACIÓN DE LAS TARJETAS DE IDENTIFICACIÓN

4.5.1 Seguridades de la tarjeta de identificación

La nueva cédula tiene 13 seguridades de alta tecnología.

Figura 27. Seguridades Anverso Cédula

Fuente: (Dirección General de Registro Civil, Identificación y Cedulación, 2010)

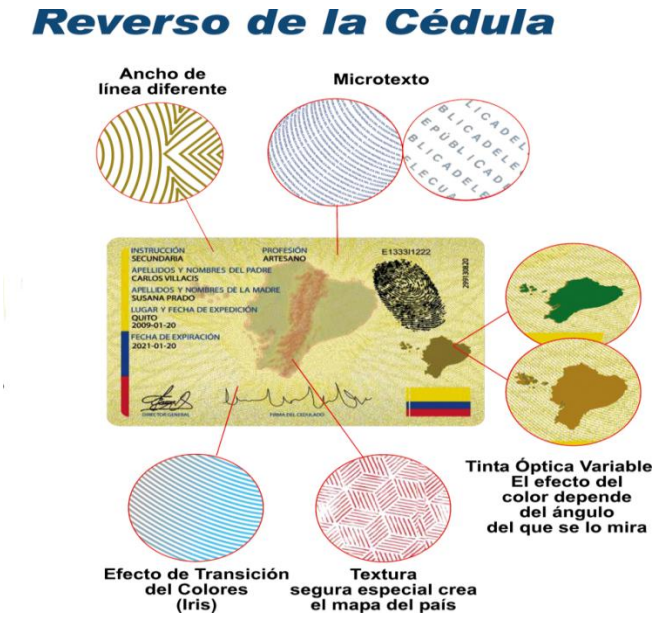


Figura 28. Seguridades Reverso Cédula

Fuente: (Dirección General de Registro Civil, Identificación y Cedulación, 2010)

La nueva cédula además ofrece seguridad en la información dado el chip donde se guarda el respaldo magnético.

4.5.2 Normas y requisitos físicos de la tarjeta de identidad

1. La tarjeta electrónica cumple con la norma ISO /IEC 7810 (Identification cards — Physical characteristics) norma que define las características físicas para tarjetas de identificación y la norma ISO/ IEC 15457-1 (Identification cards -- Thin flexible cards -- Part 1: Physical characteristics).
2. La durabilidad de la tarjeta electrónica en bodega es de 7 a 10 años.
3. La cédula de identidad electrónica cumple con la norma ISO/IEC 14443-1 Clase 1 Tarjetas de identidad - tarjetas de circuito (s) integrado Sin contacto - tarjetas de Proximidad y los correspondientes procedimientos de pruebas ISO/IEC 10373-6, RFID.

4.5.3 Especificaciones del chip:

El chip está integrado en la tarjeta electrónica conforme a las siguientes especificaciones:

1. El chip cumple con el nivel EAL 5 + EAL4+ de Evaluación de la Garantía de Seguridad de acuerdo con la norma ISO/IEC 15408 Common Criteria.
2. El sistema operativo cumple con el Nivel 4 aumentado de la evaluación de la garantía de seguridad (EAL 4+).

Los niveles de garantía de la evaluación (EAL) son paquetes predefinidos de garantía. Un EAL es conjunto básico de requisitos de garantía para la evaluación. Cada EAL define un conjunto consistente de requisitos de garantía. Juntos los EAL forman un conjunto ordenado que es la escala de garantía predefinidas de la norma.

EAL1 Funcionalmente probado

EAL2 Estructuralmente probado

EAL3 Metódicamente probado y comprobado

EAL4 Metódicamente diseñado, probado y revisado

EAL5 Semiformalmente diseñado y probado

EAL6 Diseño verificado y probado semiformalmente

EAL7 Diseño verificado y probado formalmente.

De acuerdo con la norma el chip garantiza:

El nivel EAL4 (Metódicamente diseñado, probado y revisado): nos indica que el desarrollador del chip alcanza la máxima garantía de ingeniería de seguridad positiva basada en buenas prácticas de desarrollo comercial, las cuales, aunque rigurosas, no requieren del conocimiento especializado substancial, destreza, ni otros recursos. En este caso, el análisis se apoya en el diseño de bajo nivel de los módulos del producto y se realiza búsqueda de vulnerabilidades independiente de las pruebas realizadas por el desarrollador. Los controles de desarrollo se apoyan en un modelo de ciclo de vida de desarrollo, identificación de las herramientas utilizadas y gestión de configuración automatizada.

El nivel EAL5 (Semiformalmente diseñado y probado): nos indica que el desarrollador del chip alcanza la máxima garantía de ingeniería de seguridad positiva mediante la aplicación moderada de técnicas de ingeniería de seguridad. La confianza se apoya, en este caso, en un modelo formal y una presentación semiformal de la especificación funcional y el diseño de alto nivel. La búsqueda de vulnerabilidades asegura la resistencia relativa a los ataques de penetración.

4.5.4 Características electromagnéticas, químicas, físicas y mecánicas

- OACI Doc 9303- Documentos de viaje de lectura mecánica.
- ISO/ IEC 1443 - Tarjetas de identificación - Tarjetas de circuito integrado sin contacto - tarjetas de proximidad.
- OACI NTWG, Informe Técnico del uso de circuitos integrados sin contacto en documentos de viaje de lectura mecánica.

El chip contiene información electrónica sobre el ciudadano en formato que permite al documento de identidad cumplir con las normas electrónicas de documentos de viaje ICAO 9303.

La información se organiza mediante una estructura de datos lógicos (LDS) de la aplicación de la OACI

- Las tarjetas electrónicas cumplen con las pruebas Golden Reader de la OACI con capacidad de probar pasaportes o cédulas de identidad.
- BAC - Control de Acceso Básico

  La aplicación de IS usada es [D2 18 00 00 01 10 01], los campos siguen el formato TLV (Rotulo-Lardo -*Valor), según las especificaciones de la norma OACI 930.

  El Control de Acceso Básico (BAC) se utiliza con el fin de prevenir la intercepción y captura de las [PKI] (Infraestructura de Clave Pública). Los mecanismos de control permiten que los datos almacenados en el chip sean leídos de manera segura.
- La tarjeta inteligente usa frecuencia radiales (RFID).
- Los chips son cargados durante la producción con los números seriales y claves criptográficas para BAC (Control de Acceso básico / "Basic Access Control") de la OACI. Los números de serie se proveen en formato compatible con el sistema de inventario o el sistema de manejo del chip (CMS). En general es un formato CSV estándar.
- El chip de RFID respalda tasas de datos de 848 kbps y 424 kbps en el interface de RF.
- La antena cumple con lo establecido en la norma ISO/ IEC 14443

- La tarjeta electrónica con y su chip cumplen con la parte 3 de la Norma ISO 14443.
- La tarjeta electrónica contiene un chip seguro sin contacto que permite que la identidad electrónica pueda ser leída por lectores según la norma ISO/IEC 14443, lectores que pueden seleccionar un AID para el eID y otros AIDs que sean necesarios para otras aplicaciones existentes.
- Cumple pruebas de conformidad con ISO 14443.
- Las características de transferencia de poder de acoplamiento inductivo cumple con los estándares para la frecuencia y el volumen de operación del campo magnético conforme a las disposiciones de la Norma ISO/IEC 14443.
- La distancia de lectura, conforme al documento 9303 de la OACI, es de un máximo de 5cm.
- La interfaz de comunicación soporta tipo A y tipo B. La activación de la interfaz y las características anti colisión, los métodos, normas utilizados para el acoplamiento del campo magnético, los bits de formato de código 7 bytes, oferta de comandos (REQ) y respuesta a la petición (ATQ) deben cumplir la norma 14443 ISO / IEC.
- La tasa nominal de transferencia de datos entre el lector y el chip soporta 424 Kbits /s y 848 kbits/s.
- La arquitectura de los chips RFID cumplen al menos 50 Megaciclos de lectura/escritura sin errores.
- EAL 5+ con la prueba del certificado.
- Cuenta con los recursos de una sola escritura / muchas lecturas
- Capacidad de retención de datos de 7 a 10 años.
- La aplicación ICAO debe soportar EAC, BAC, AA, PA
- El chip tiene al menos 128KB de memoria EEPROM y más de 80KB luego de la personalización. Almacenamiento de datos para:
    a) Dos imágenes de huella digital.
    b) Según la norma OACI una huella digital WSQ (del pulgar derecho e izquierdo) y al menos dos puntos característicos de las huellas dactilares (ambos índices) según ANSI INCITS 378, y hasta diez minucias a futuro.

c) La imagen facial.
d) Las claves criptográficas y sus certificados relacionados (y la cadena de certificados para verificaciones).

- La aplicación LDS (Logical Data Structure) del chip cumple con la norma 9303 de la OACI (Definición de grupos de datos para documentos de viaje).
- El hardware que soporta la infraestructura de los algoritmos de clave pública/privada permite la muestra en el documento OACI 9303, como mínimo:
    a) Todas las recomendaciones de los mínimos tamaños de clave en relación con países claves de firma de Entidades de Certificación (CA), llaves firmantes del documento y claves de autenticación de Active Authentication.
    b) Utilización de triple DES y AES.
    c) Los algoritmos hash es el especificado en el Documento OACI 9303 de la OACI.
    d) 128KB EEPROM como mínimo.
    e) La estructura de los grupos de LDS de datos siguen la norma de OACI 9303, y contienen al menos los grupos de datos siguientes:
        - EF.COM;
        - DG1- MRZ (con todos los elementos de datos) - BAC /AA;
        - DG2- Cara (JPEG) - BAC /AA;
        - DG3 FingerPrint (WSQ)
        - DG14 - Educación y Cultura.
        - DG15. AA;
        - EF.SOD - hash y firma digital
    f) Pruebas de interoperabilidad lector / OACI con el chip.
    g) El chip y la antena no son visibles en la capa de soporte al usuario.
    h) La integridad, autenticidad y confidencialidad de los datos almacenados digitalmente están de acuerdo con la OACI NTWG, PKI para los documentos de viaje de lectura mecánica conforme ICC Lectura-* Solo acceso.

- Contiene segmentos múltiples y AIDs que pueden requerir diferentes mecanismos de autenticación. El chip y su sistema operativo, por lo tanto proveen estos mecanismos y protocolos, tienen la capacidad de segmentar el chip para permitir la lectura, escritura y reescritura.
- Aplicaciones

  Aplicaciones OACI LDS con soporte BAC, EAC

  El sistema operativo del chip es capaz de respaldar futuros segmentos de memoria que no sean de la OACI (dirigidos a la aplicación individual de IDs - AID) para fines especiales como:

  a) Aplicaciones de ePKI, X.509, RSA(PKCS#1), Perfil (PKCS#15), Soporte a CWA 14890 -1, -2; Autenticación (interna y externa) conforme a ISO 17816 -4 y -8; Estándar de Firma Digital (DSS) FIPS 186-2.
  b) Verificación de huella digital en tarjeta (MoC)
  c) Contiene al menos 5 monederos electrónicos.
  d) Aplicación de epicrisis, conforme a los estándares internacionales
  e) Software de interacción que permite interactuar con las aplicaciones de la tarjeta incluido su manual de funcionamiento.
- Requisitos de cifrado.

  En lo que concierne a los requisitos de criptografía para el chip y el sistema operativo con respecto al cifrado simétrico ejecuta y gestiona una sesión completa de mensajería segura, según lo definido por la OACI para las sesiones BAC (conforme a Doc. de OACI 9303, Parte 1, Volumen 2) y, con respecto al cifrado asimétrico ejecuta y gestiona una sesión de autenticación activa de OACI en cifrado RSA de 2048 bits y SHA hasta 512.
- La seguridad de la tarjeta electrónica y su resistencia a la falsificación se basan en los siguientes requerimientos generales: autenticación (interna y externa) conforme a ISO 7816 -4 y -8.

4.6 ESTADÍSTICAS DE PÉRDIDA DE DOCUMENTOS PERSONALES Y FALSIFICACIÓN DE FIRMA O DOCUMENTOS

4.6.1 Distrito Metropolitano de Quito

De acuerdo con el informe17 de seguridad ciudadana 2012 del Observatorio Metropolitano de Seguridad Ciudadana (OMSC) del Municipio del Distrito Metropolitano de Quito se presentan las siguientes estadísticas:

4.6.1.1 Asalto y robo a personas

Cuadro 4.

Estadísticas de Asalto y robo a personas en Quito

	FRECUENCIAS		PORCENTAJES		TASAS POR CADA 100 MIL HAB.	
Año	**2011**	**2012**	**2011**	**2012**	**2011**	**2012**
Total	6.257	7.950	100%	100%	264,5	329,5

Fuente: (Observatorio Metropolitano de Seguridad Ciudadana, OMSC, 2013)

Para el año 2012 en segundo lugar de los objetos más robados se encuentran los objetos y documentos personales con un porcentaje de 44.8%.

4.6.1.2 Robo a personas

Cuadro 5.

Estadísticas de Robo a personas en Quito

	FRECUENCIAS		PORCENTAJES		TASAS POR CADA 100 MIL HAB.	
Año	**2011**	**2012**	**2011**	**2012**	**2011**	**2012**
Total	5.558	6.663	100%	100%	234,9	276,2

Fuente: (Observatorio Metropolitano de Seguridad Ciudadana, OMSC, 2013)

En esta modalidad para el año 2012 en segundo lugar de los objetos más robados son los objetos o documentos personales con un porcentaje 35,2%.

4.6.1.3 Hurto a personas

Cuadro 6.

Estadísticas de Hurto a personas en Quito

	FRECUENCIAS		PORCENTAJES		TASAS POR CADA 100 MIL HAB.	
Año	**2011**	**2012**	**2011**	**2012**	**2011**	**2012**
Total	1.167	1.413	100%	100%	49,3	58,6

Fuente: (Observatorio Metropolitano de Seguridad Ciudadana, OMSC, 2013)

De acuerdo al tipo de objeto sustraído, los objetos o documentos personales ocupan el 21,0%.

4.6.2 Guayaquil

De acuerdo con los informes anuales de "PRINCIPALES DELITOS CONTRA LAS PERSONAS Y CONTRA LA PROPIEDAD" denunciados en el Ministerio Fiscal en la ciudad Guayaquil del Centro de Estudios e Investigaciones Estadísticas FCNM-ESPOL de los años 2009, 2010, 2011,2012, se presentan las estadísticas de la falsificación de firma o documentos y pérdida de documentos.

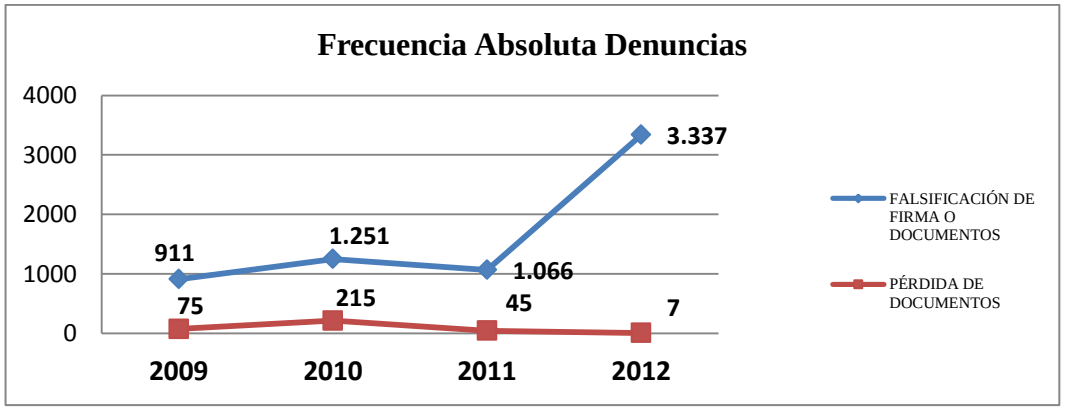


Figura 29. Estadísticas de Falsificación de firma o documentos y perdida de documentos – Guayaquil

Fuente: (Centro de Estudios e Investigaciones Estadísticas FCNM-ESPOL, 2013)

De acuerdo con los informes antes indicados se puede apreciar que los documentos personales ocupan el segundo lugar de objetos más robados en los asaltos, robos y hurtos a personas en el año 2012 y la falsificación de firma o documentos se ha duplicado en el mismo año.

4.7 ESTADÍSTICAS DE USO (REAL) DEL DNI ELECTRÓNICO EN ESPAÑA

En el informe de Indicadores del Observatorio de Administración Electrónica (ANGELBORROY, 2012) de junio de 2012 se presentan datos sobre DNIe y firma electrónica:

Ciudadanos con DNIe = 28.532.108

Validaciones de firma e identidad electrónica = 66.808.740 (consultas registradas en Plataforma de Validación @firma)

4.7.1 Ciudadanos con DNIe

Algunos factores a tener en cuenta:

- No todos los DNI electrónicos emitidos incluyen la generación del certificado en la tarjeta criptográfica.
- No todas las personas que tienen un DNI electrónico con el certificado generado conocen la clave de utilización.
- No todos los ciudadanos disponen de un ordenador configurado (drivers y lector de tarjetas) para poder usar el DNI electrónico.
- Los certificados del DNI electrónico caducan cada 20 meses y requieren renovación presencial en las oficinas de la Policía, por lo que algunos certificados generados no pueden emplearse.
- Si descontamos de la cifra de 28 millones todos los DNIe que se encuentren bajo alguno de los anteriores supuestos, la cifra de certificados activos y en condiciones de uso disminuye drásticamente.

4.7.2 Validaciones de firma e identidad electrónica

En el caso de las validaciones, debe considerarse:

La Plataforma de Validación @firma es empleada solo por una parte de la Administración Pública, ya que existen organismos que se conectan directamente a las Autoridades de Validación del DNIe.

La Plataforma de Validación @firma no solo valida DNIe, sino que incluye soporte para 23 tipos de certificados adicionales.

Para una misma operación puede requerirse más de una validación del certificado, como en el caso de los formatos de firma avanzada recomendados por el Esquema Nacional de Interoperabilidad - ENI.

De acuerdo con la encuesta sobre equipamiento y uso de tecnologías de la información y comunicación en los hogares 2010 realizado por el Instituto Nacional de Estadísticas, las personas que disponen de algún certificado de firma electrónica (DNIe u otro) por Comunidades Autónomas y uso de los mismos en sus relaciones con las administraciones públicas a través de Internet se presenta a continuación (INE Instituto Nacional de Estadísticas, 2010):

Cuadro 7.

Estadísticas de certificado de firma electrónica DNIe de España

	Total de persona que disponen de algún certificado de firma electrónica (DNIe u otro)	Uso de los mismos en sus relaciones con la AA.PP a través de Internet: DNI electrónico	Uso de los mismos en sus relaciones con las AA.PP a través de Internet: Otros certificados de firma electrónica reconocidos
Total Nacional	**11.534.046**	**4.7%**	**13.0**

Fuente: (INE Instituto Nacional de Estadísticas, 2010)

4.8 DISPOSITIVOS DE ALMACENAMIENTO DE CERTIFICADOS DIGITALES TARJETA CRIPTOGRÁFICA, TOKEN USB

4.8.1 Tarjeta Criptográfica de la cédula

4.8.1.1 Ventajas:

- El chip criptográfico contiene un microprocesador que realiza las operaciones criptográficas con la clave privada.
- La clave nunca se expone al exterior.
- Doble seguridad: posesión de la tarjeta y PIN de acceso.
- Chip criptográfico de acceso por radiofrecuencia.

4.8.1.2 Desventajas:

- Se precisa de un middleware.

- Requiere un lector USB de radiofrecuencia RFID.
- Se requiere de un chip SAM para la autenticación criptográfica entre la tarjeta y el lector.
- Las operaciones criptográficas son lentas, lo que exige mantener la proximidad un tiempo significativo.
- (CSP) específico para utilizar la tarjeta.
- El número de certificados que se pueden cargar depende del perfil de certificado, de la capacidad del chip y del espacio que se reserve para los certificados.

4.8.2 Token USB

Al igual que las tarjetas criptográficas sirven de almacén de claves/certificados y realizan las operaciones criptográficas en su interior.

4.8.2.1 Ventajas:

- No precisan de lector (sólo puerto USB), reducido tamaño.
- (Dispositivo seguro USB), ideal para transacciones en donde el usuario a través de una clave de mínimo 8 dígitos (PIN Token).

4.8.2.2 Desventaja

- No sirven como tarjeta de identificación.

Como se puede apreciar el uso de la cedula como dispositivo de almacenamiento de certificados digitales presenta desventajas para la implementación del servicio de firma electrónica.

4.9 INFRAESTRUCTURA FIRMA ELECTRÓNICA ECUADOR

De acuerdo con la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos su Reglamento y la nueva Ley de Telecomunicaciones la ARCOTEL es la entidad que autoriza la acreditación de Entidades de Certificación de Información y Servicios Relacionados, es responsable de la organización y funcionamiento del Registro Público de Entidades de Certificación de Información y Servicios Relacionados además de realizar los controles necesarios a las Entidades de Certificación así como a los terceros vinculados, con el objeto de garantizar el

cumplimiento de la normativa vigente y de los términos y condiciones de autorización y registro.

En el Ecuador existen 4 Entidades de Certificación de Información y Servicios Relacionados: Banco Central del Ecuador, ANF Autoridad de Certificación, Security Data y Concejo de la Judicatura, cada una con su propia infraestructura de clave pública.

El Banco Central del Ecuador mediante convenio (tercero vinculado) firmado con la Dirección General de Registro Civil, Identificación y Cedulación se encuentra expandiendo el servicio de firma electrónica (certificados digitales) a nivel provincial donde no tiene presencia. La DIGERCIC se encuentra desempeñando las funciones de Autoridad de Registro de la Entidad de Certificación del Banco Central y brinda los servicios correspondientes a la emisión, renovación y revocación de certificados digitales para personas naturales, jurídicas y funcionarios públicos, servidor Web así como soporte informativo a usuarios.

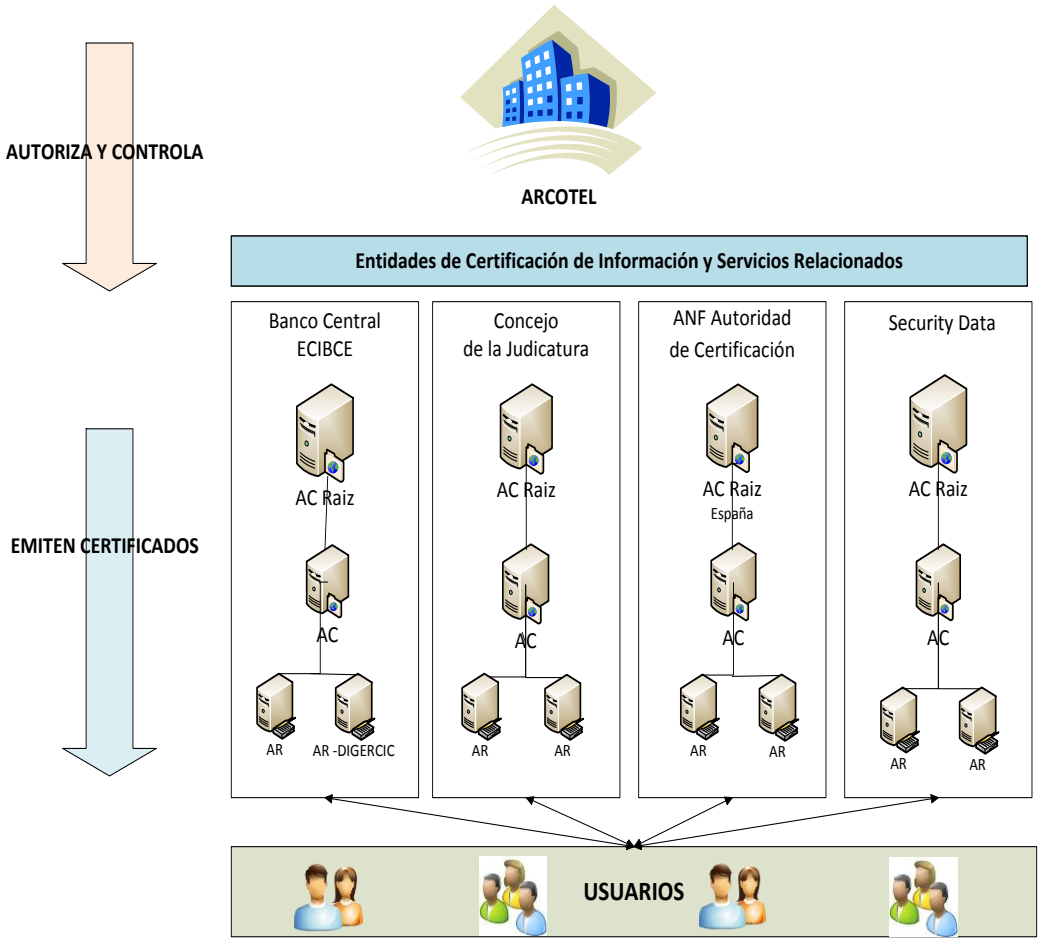


Figura 30. Infraestructura Actual de Firma Electrónica Ecuador

A continuación se presentan las estadísticas de firma electrónica en el Ecuador de acuerdo con el reporte publicado por la Agencia de Regulación y Control de Telecomunicaciones el 20 de marzo de 2015.

Tabla 14.

Número de certificados emitidos, revocados y vigentes

No.	CERTIFICADOS	2009	2010	2011	2012	2013	2014	2015-FEBRERO
1	EMITIDOS	2.365	5.155	8.658	33.275	52.563	88.445	**94.717**
2	REVOCADOS	192	1.087	2.199	3.929	8.636	22.351	24.933
3	VIGENTES	2.173	4.068	6.459	29.346	43.927	66.094	69.784

Fuente: (Agencia de Regulación y Control de Telecomunicaciones, 2015)

Tabla 15.

Número de certificados emitidos, revocados y vigentes por provincia

No.	CONCESIONARIO	EMITIDOS	REVOCADOS	VIGENTES
1	AZUAY	**5.560**	1210	4350
2	BOLIVAR	**257**	68	189
3	CAÑAR	**472**	91	381
4	CARCHI	**708**	180	528
5	CHIMBORAZO	**1.294**	373	921
6	COTOPAXI	**915**	156	759
7	EL ORO	**3.351**	651	2700
8	ESMERALDAS	**661**	159	502
9	GALAPAGOS	**331**	81	250
10	GUAYAS	**26.473**	6600	19873
11	IMBABURA	**1.739**	396	1343
12	LOJA	**1.627**	308	1319
13	LOS RIOS	**684**	103	581
14	MANABI	**2.702**	656	2046
15	MORONA SANTIAGO	**293**	79	214
16	NAPO	**201**	54	147
17	ORELLANA	**240**	40	200
18	PASTAZA	**297**	72	225
19	PICHINCHA	**41.958**	12637	29321
20	SANTA ELENA	**465**	126	339
21	SANTO DOMINGO	**1.054**	180	874
22	SUCUMBIOS	**437**	68	369
23	TUNGURAHUA	**2.588**	577	2011
24	ZAMORA CHINCHIPE	**188**	43	145
25	OTROS	**222**	25	197
TOTAL		**94.717**	**24.933**	**69.784**

Fuente: (Agencia de Regulación y Control de Telecomunicaciones, 2015)

Tabla 16.

Número de certificados emitidos, revocados y vigentes por entidad de certificación

No.	CERTIFICADOS	BCE	SD	ANF	CDJ	TOTAL - FEB 2015
1	EMITIDOS	**61.820**	**31.996**	**304**	**597**	**94.717**
2	REVOCADOS	14.816	10.071	41	5	24.933
3	VIGENTES	47004	21925	263	592	69.784

Fuente: (Agencia de Regulación y Control de Telecomunicaciones, 2015)

4.10 ANÁLISIS DE FORTALEZAS, OPORTUNIDADES, DEBILIDADES Y AMENAZAS DIGERCIC

A continuación se presenta el análisis de la situación actual de la DIGERCIC identificando fortalezas, debilidades, oportunidades y amenazas para tomar decisiones sobre la implementación del servicio de firma electrónica por la DIGERCIC

4.10.1 Evaluación interna

Se evaluaron las fortalezas y debilidades más importantes de la DIGERCIC, teniendo como objetivo sacar provecho de las fortalezas y superar las debilidades.

Tabla 17.

Fortalezas y Debilidades - DIGERCIC

FORTALEZAS		DEBILIDADES	
F1	Agencias con cobertura a nivel nacional con presencia en las 24 provincias y a nivel cantonal.	**D1**	Personal técnico y operativo no capacitado para brindar el servicio de firma electrónica.
F2	Infraestructura tecnológica modernizada.	**D2**	La DIGERCIC no posee certificación ISO 27001.
F3	La DIGERCIC dispone de una cantidad suficiente de Tarjetas de Identificación con capacidad para soportar el servicio de firma electrónica.	**D3**	No cuenta con recursos suficiente para la inversión en el proyecto de firma electrónica.
F4	La DIGERCIC dispone del Sistema MAGNA con capacidad para soportar base de datos a nivel nacional.	**D4**	Usuarios de firma electrónica requieren un lector RFID con SAM para lectura del chip de la cédula de identidad.
F5	Talento Humano renovado – joven.	**D5**	Retraso en los procesos de adquisición de insumos y consumibles.
F6	Autoridades comprometidas.	**D6**	Dependencia de proveedor del sistema MAGNA para la implementación y desarrollo de los sistemas para la integración del servicio de firma electrónica.

Estrategias.

Reingeniería de la DIGERCIC que permita desarrollar nuevos servicios electrónicos (servicios e goverment) agregadores de valor como el servicio de firma electrónica con el apoyo de una unidad de investigación y desarrollo de las TIC y la obtención de la Certificación ISO 27001.

4.10.2 Evaluación externa

Se evaluaron las oportunidades y amenazas más importantes de la DIGERCIC, teniendo como objetivo realizar un reconocimiento del ambiente externo o entorno que la rodea para aprovechar las oportunidades y eludir los riesgos.

Tabla 18.

Oportunidades y Amenazas - DIGERCIC

	OPORTUNIDADES		AMENAZAS.
O1	Nuevos Servicios que usan firma electrónica en el Ecuador (Quipux, Ecuapass, Factura Electrónica).	**A1**	Altos costos de insumos y consumibles requeridos para la implementación del servicio de firma electrónica.
O2	Políticas Gubernamentales que incentivan la investigación, desarrollo e innovación I+D+I en Tecnologías de la Información y Comunicación.	**A2**	Intereses de otros sectores tales como el Banco Central para mantener el control de la firma electrónica.
O3	Demanda del servicio de firma electrónica en zonas geográficas donde no tiene presencia las actuales entidades certificadoras.	**A3**	Competencia desleal de Entidades de Certificación Acreditadas, ANF, Security Data y Banco Central.
O4	Nuevas competencias para la DIGERIC (la emisión de pasaporte electrónico requiere el uso de firma electrónica).	**A4**	Ingreso de nuevas entidades de certificación (como el Concejo de la Judicatura)
O5	Políticas Gubernamentales para el desarrollo del gobierno electrónico en el Ecuador.		
O6	Alianzas estratégicas con entidades de Estado tales como el Banco Central, Municipios, DINARDAP.		

Estrategias.

Establecer sinergias con entidades que desarrollen estrategias vinculadas con la reforma del Estado para impulsar la reforma a la Ley de Comercio Electrónico y Mensajes de Datos, Firma Electrónica creando un modelo jerárquico de Autoridades de Certificación a nivel nacional.

Impulsar y fortalecer las relaciones interinstitucionales con organismos del estado y similares internacionales para gestionar servicios.

CAPÍTULO V

PROPUESTA TÉCNICA

En base a los resultados obtenidos en el análisis FODA para el servicio de firma electrónica se presentan una propuesta para la implementación del servicio de firma electrónica por parte de la DIGERCIC.

5.1 INFRAESTRUCTURA DE FIRMA ELECTRÓNICA PARA LA REPÚBLICA DEL ECUADOR

Se plantea reformar la Ley de Comercio Electrónico y Mensajes de Datos, Firma Electrónica y su reglamento para crear un modelo jerárquico de Infraestructura de Firma Electrónica para la república del Ecuador siendo de aplicación para la prestación de servicios de certificación electrónica tanto por el sector público como el privado. Así como reformar la Ley General de Registro Civil, Identificación y Cedulación para asignar nuevas funciones y atribuciones a la DIGERCIC.

La Infraestructura estaría compuesta por:

a. Entidad de Acreditación y Control de Certificación Electrónica (EACCE)
b. Autoridad de Certificación Raíz del Ecuador (ACREC)
c. Entidades de Certificación de Información y Servicios Relacionados (EC)
d. Usuarios
e. Terceros usuarios

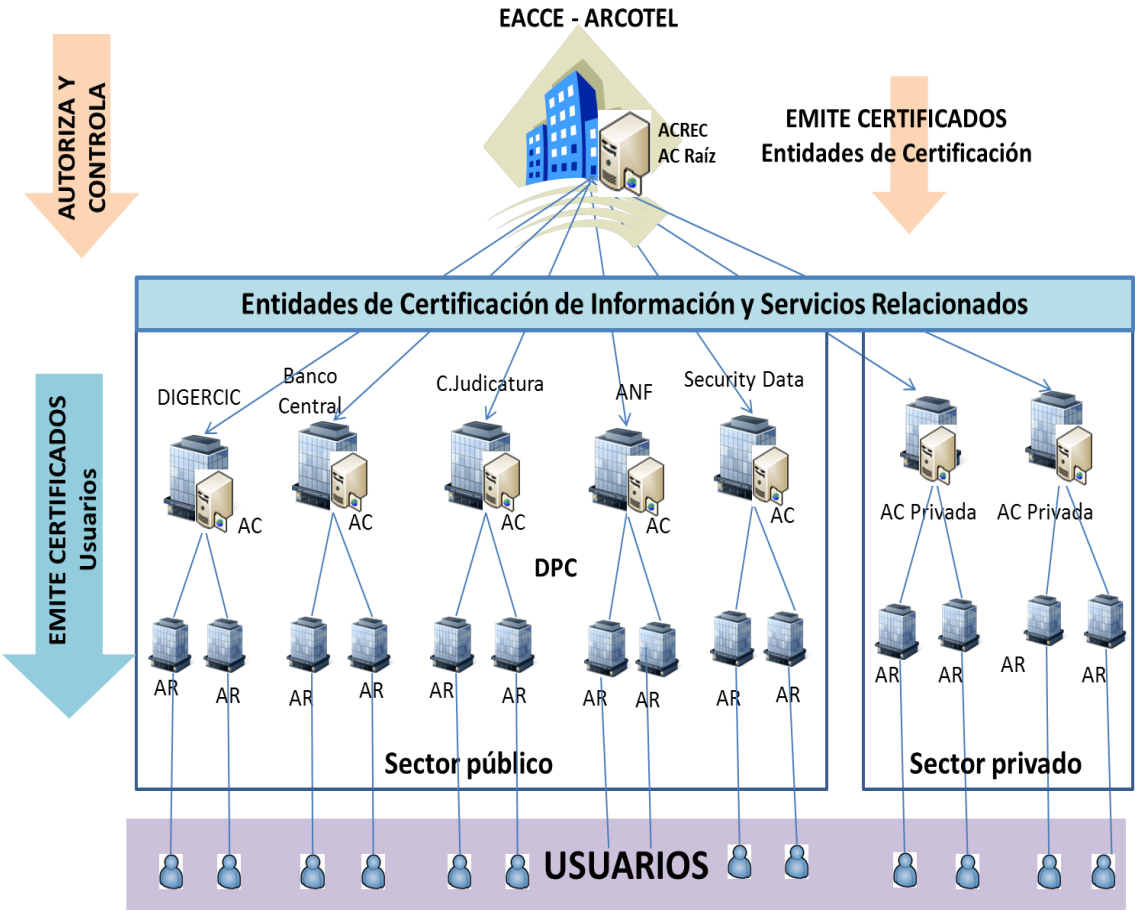


Figura 31. Modelo Infraestructura Nacional de Certificación Electrónica a nivel jerárquico

5.1.1 Entidad de Acreditación y Control de Certificación Electrónica (EACCE)

Las funciones de la Entidad de Acreditación que se plantean son:

De Acreditación:

- Recibir, tramitar y resolver las solicitudes de acreditación para Entidades de Certificación.
- Inscribir a las Entidades de Certificación en el Registro Público de Entidades de Certificación de Información y Servicios Relacionados acreditadas.
- Modificar, suspender o revocar la acreditación de Entidades de Certificación acreditadas.

- Mantener en el sitio web de la Entidad de Certificación Electrónica, la información relativa al Registro de Entidades de Certificación Acreditadas, tales como altas, bajas, sanciones y revocaciones.

De control:

- Controlar la calidad y confiabilidad de los servicios brindados por las Entidades de Certificación acreditadas así como los procedimientos de auditoría que se establezcan en la normativa.
- Realizar auditorías a las Entidades de Certificación acreditadas, de conformidad con los criterios que la normativa establezca para verificar todos los aspectos relacionados con el ciclo de vida de los certificados y de sus claves criptográficas.
- Determinar las medidas que estime necesarias para proteger la confidencialidad de los titulares de certificados.
- Efectuar inspecciones y requerir en cualquier momento a las Entidades de Certificación acreditadas toda la información necesaria para garantizar el cumplimiento de la función en los términos definidos en las leyes y sus reglamentos.

De regulación:

- Definir los estándares técnicos y operativos que deberán cumplir las Entidades de Certificación acreditadas, así como los procedimientos y requisitos de acreditación necesarios para su cumplimiento.
- Fijar reglas y patrones de la industria que aseguren la compatibilidad, interconexión e interoperabilidad, así como el correcto y seguro funcionamiento de los dispositivos de creación y verificación de firma, controlando su aplicación.

De sanción:

- La Entidad de Acreditación y Control podrá imponer a las Entidades de Certificación acreditadas que infringiere total o parcialmente cualquiera de las obligaciones derivadas de las leyes o de las normas que resulten aplicables al servicio que presten, las sanciones se aplicarán de acuerdo con la gravedad o reiteración de la infracción (AGESIC, Agencia de gobierno electrónico y sociedad de la informacion, sf).

5.1.2 Autoridad de Certificación Raíz del Ecuador (ACREC)

Autoridad de Certificación Raíz administrada por la Entidad de Acreditación y Control de Certificación Electrónica - SENATEL/ARCOTEL3; constituirá la única instalación de su tipo y revestirá la mayor jerarquía de la Infraestructura de Firma Electrónica de la Republica de Ecuador. Emitirá los certificados digitales a las Entidades de Certificación de Información y Servicios Relacionados acreditadas, una vez aprobados los requisitos de acreditación.

Definirá la Política de Certificación y Declaración de Prácticas de Certificación (CPS) para la operación de la infraestructura de Firma Electrónica de la República del Ecuador.

5.1.3 Entidades de Certificación de Información y Servicios Relacionados (EC)

Las Entidades de Certificación de Información y Servicios Relacionados (EC) estarán constituidas por su propia Infraestructura de Clave Pública donde la Autoridad de Certificación será subordinada a la Autoridad de Certificación Raíz del Ecuador.

Dentro de sus principales funciones son la emisión, modificación, revocación o suspensión de Certificados Digitales a usuarios finales. Las Entidades de Certificación no podrán emitir certificados a otras Entidades de Certificación.

5.1.4 Usuarios

Los usuarios son personas físicas, jurídicas o aplicaciones, especificando para este último caso si se trata de sitios seguros.

5.1.5 Terceros usuarios

Son terceros usuarios de los certificados emitidos, toda persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente.

---

[3] Durante el desarrollo de la tesis se encontraba en discusión y aprobación la nueva Ley de Telecomunicaciones, donde se creará a la Agencia de Regulación y Control de Telecomunicaciones –ARCOTEL.

5.1.6 Diagrama de Flujo del proceso de certificación electrónica

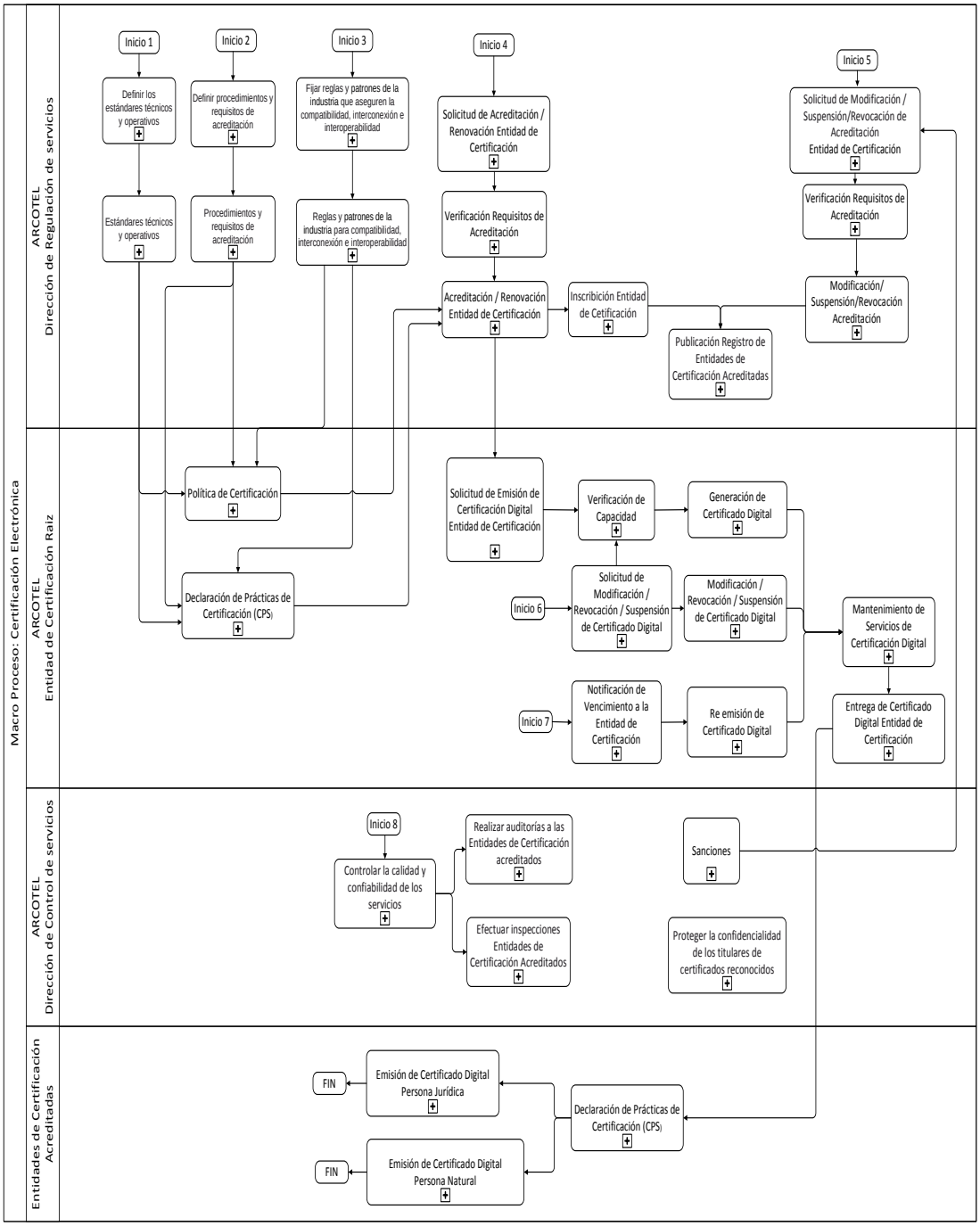


Figura 32. Diagrama de Flujo del proceso de certificación electrónica

5.2 Arquitectura PKI DIGERCIC

Para la definición de la arquitectura de la estructura de certificación se considera que la DIGERCIC asumirá la competencia de la emisión de pasaportes por lo que, la DIGERCIC al momento de implementar este servicio debe tomar en cuenta

la estructura PKI recomendada por la OACI para la emisión de pasaportes electrónicos.

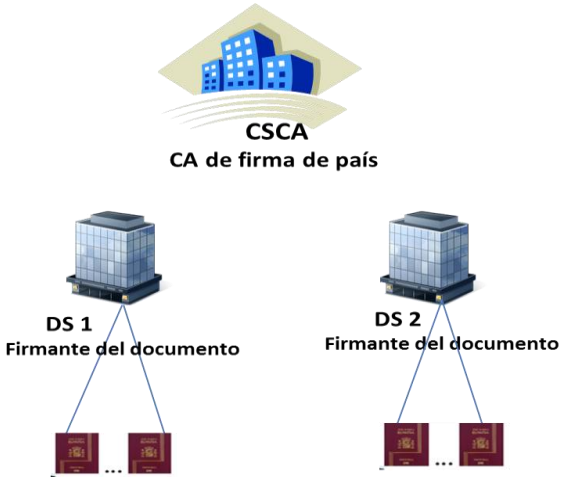


Figura 33. Estructura PKI recomendada por la OACI para la emisión de pasaportes electrónicos

Fuente: (OACI Organización de Aviación Civil Intenacional, 2008)

La OACI para el periodo de expedición de la clave de CA de firma de país recomienda que la clave de la CA de firma de país sea sustituida cada 3 a 5 años (Organización de Aviación Civil Internacional- OACI, 2008) y el periodo de expedición de clave del firmante de documentos máximo en que se utilice la clave del firmante de documentos para firmar dvLM (OACI Organización de Aviación Civil Intenacional, 2008) sea de 3 meses, los certificados se emiten con periodos de validez muy cortos que requieren frecuentes renovaciones. Los periodos de validez de las claves de una AC Raíz y AC Subordinada en una infraestructura de clave pública tradicional son de 20 a 30 años como máximo. Debido a la considerable diferencia en los periodos de validez de las claves y certificados de la PKI para el servicio de firma electrónica y el servicio de pasaportes electrónicos se requiere implementar dos estructuras PKI una para cada servicio. La arquitectura PKI para el servicio de pasaporte electrónico no es parte de este trabajo.

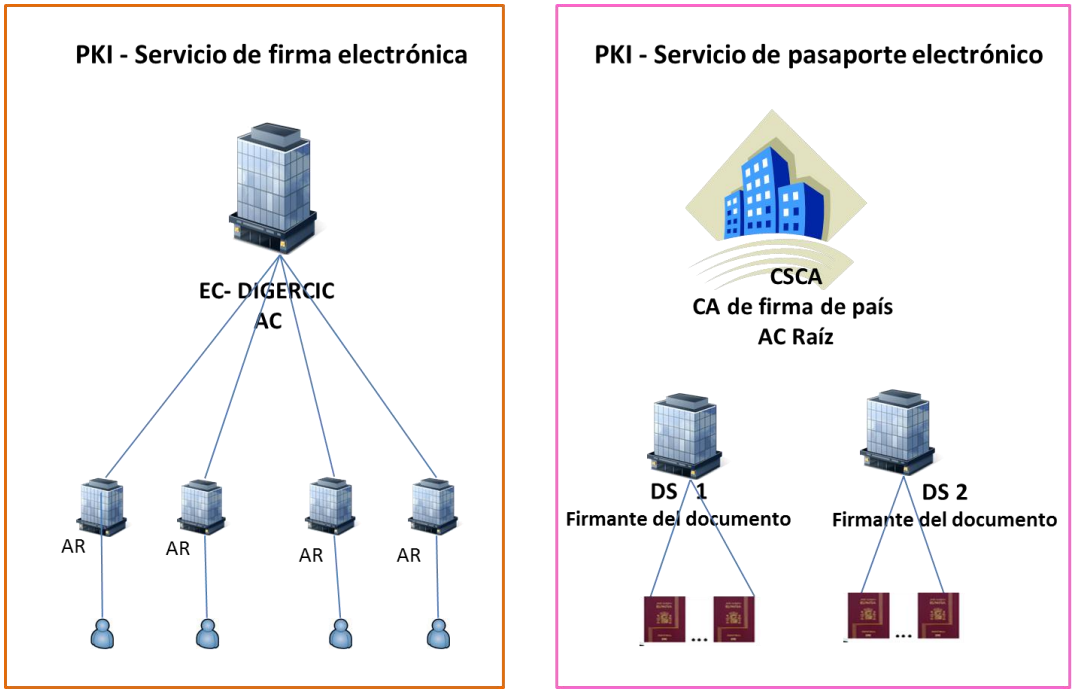


Figura 34. Modelo PKI DIGERCIC

5.3 AUTORIDAD DE CERTIFICACIÓN PKI PARA EL SERVICIO DE FIRMA ELECTRÓNICA

La Infraestructura de clave pública debe cumplir con las siguientes especificaciones:

5.3.1 Atributos operativos de la autoridad AC

- Emitir indeterminado número de certificados.
- Emitir certificados que cumplan con los estándares X.509 v.3.
- Generar y procesar solicitudes de certificados en formato PKCS#10.
- Generación de certificados y CRLs conformes al RFC 5280.
- Una extensión con los puntos de distribución de la CRL. Soporte mínimo de urls HTTP y LDAP para especificar la ubicación de la CRL. Debe poder especificarse un OCSP responder en la extensión: Authority Information Access.
- Generar todas las extensiones obligatorias.
- La AC deben poder definir diferentes perfiles de certificados.
- Soportar extensiones privadas en los certificados.

- Soportar al menos uno de los siguientes algoritmos para firmar digitalmente los certificados y CRLs: RSA, DSA.
- Soporte para conexión con dispositivos criptográficos cumpliendo con RSA PKCS#11 (USB).
- Generar de forma automática (configurable) o manual CRLs, las que deben cumplir con el estándar X.509 v.2
- Manejar automáticamente los CDPs (CRL Distribution Point), configurables para publicar periódicamente la CRL.
- ITU-T X.509v2 CRL simple y múltiples puntos de distribución.
- Los HSMs de la PKI deben permitir guardar indeterminado número de certificados en cada uno.
- La cantidad por cada servidor que conforma cada módulo de la solución propuesta son tres: producción, contingencia y un tercero para test, que deben cumplir con FIPS 140-2 nivel 3 o superior y que deberían incluir:
    - Funcionalidad de clonación, de modo que uno de los dispositivos pueda funcionar como respaldo del otro.
    - Capacidad de generar pares de claves RSA de tamaño 2048 a 4096 bits como mínimo.
    - Deben ser dispositivos de alta disponibilidad y tolerancia a fallas. Por ejemplo tiempo medio de fallas (MTBF) de acuerdo al estándar MIL Handbook 217F.

5.3.1.1 Funcionalidades para la gestión de certificados:

- Visualización de los campos del certificado, y definición de extensiones del mismo.
- Administración de los permisos sobre los usuarios que podrán emitir certificados de acuerdo a cada plantilla de perfiles
- Manejo de grupos de usuarios o roles, pudiendo asignárseles plantillas de perfiles.
- Generación y visualización de una auditoría de eventos del sistema, esta auditoría debe contener como mínimo fecha, hora, solicitante y usuario que emite el certificado.

- Herramientas para la administración de las CRLs y la declaración de prácticas y las políticas de certificación.
- Consultas sobre la vigencia de los certificados reconocidos.

5.3.1.2 Un sistema de control de acceso de la AC, el cual debe soportar:

- Al menos los siguientes roles: administrador, emisor de certificados, operador, auditor.
- Múltiples usuarios logueados simultáneamente para ejecutar determinada tarea.
- Definición de responsabilidades sobre los roles de la aplicación AC.
- También debe utilizar un mecanismo de autenticación de usuarios de dos (2) factores.
- Los distintos módulos que se integrarán en la PKI (AC, AR, AV y TSA) serán preferentemente en soluciones de hardware y software integrados en servidores independientes e interoperables para garantizar la escalabilidad y robustez de la solución.
- El centro de desarrollo de la empresa fabricante deberá estar certificado Common Criteria EAL4+ (*).

5.3.1.3 Aspectos Fundamentales:

- Modelado de políticas y mejores prácticas para la Infraestructura de Autoridad de Certificación: Autoridad de certificación subordinada, Autoridad de validación, Autoridad de sellado de tiempo y despliegue de conectores inteligente de AR, además de sus consolas y servidores de configuración.
- Cumplir con los requerimientos de hardware para la creación e implantación de las autoridades de certificación (Hardware criptográfico) sustentada sobre Módulos de Almacenamiento Criptográfico (HSM) certificados internacionalmente con FIPS 140-2 Nivel 3 y/o Common Criteria EAL4+.
- Para el sitio alterno los modelos de comunicaciones interna y externa deben ser con tolerancia a fallas.
- Modelados de protocolos en línea para la actualización de listas de revocación offline.

5.3.2 Tipo de Hardware con HSM y aplicación Software

A continuación se presentan las características generales del tipo de hardware y software para los servidores de Autoridad de Certificación Subordinada, Autoridad de Registro, Autoridad de Sellado de Tiempo y Servidor de Firma.

5.3.2.1 Características generales

a) Cantidad 3 (TRES) servidores.
b) 1U o 2U, Rack-mountable en rack
c) Procesador Intel Xenon E3-1200 o Superior
d) Velocidad CPU mínima 2,6 GHz
e) Memoria RAM mínima (instalada) 8GB y mínima (soportada) 32GB
f) Hardware criptográfico (HSM) certificado integrado
g) Tamper resistant HSM.- Características de alta seguridad física contra intrusiones y manipulaciones: Borrado automático de información sensible en caso de detección de intento de intrusión o manipulación.
h) El HSM que incluya el servidor debe permitir guardar y custodiar indeterminado número de certificados.
i) Capacidad ilimitada de generación de certificados sin coste adicional

5.3.2.2 Conectividad:

a) Puerto Serie Entrada/salida directa de HSM.
b) Puerto Serie de Servidor.
c) Doble interfaz Ethernet 10/100/1000

5.3.2.3 Algoritmos y Funciones Hash:

a) RSA soportado con longitud de clave de hasta 4.096 bit.
b) MD5.
c) SHA-1, SHA-2 hasta SHA-512.
d) RIPEMD[4] en 128 y 160 bit.

5.3.2.4 Cumplimiento de Estándares:

a) RSA PKCS#1_v1.5
b) RSA X509v3 RFC 3280.

[4] RIPEMD-160 (acrónimo de RACE Integrity Primitives Evaluation Message Digest, primitivas de integridad del resumen del mensaje) es un algoritmo del resumen del mensaje de 160 bits (y función criptográfica de hash) desarrollado en Europa por Hans Dobbertin,

c) NTP v3.0, PKCS#1, PKCS#8, PKCS#10, PKCS#12, PKCS#15, SHA, X.509v3 CRLv2 rfc3280,
d) http, https (RFC 2818 HTTP sobre TLS (HTTPS)

5.3.2.5 Certificaciones de seguridad:

a) FIPS 140-2 Nivel 3 para los dispositivos criptográficos (HSMs)
b) Common Criteria EAL4+ para los dispositivos criptográficos (HSMs).

5.3.2.6 Alta disponibilidad.

a) Capacidad de configurar los servidores bajo un esquema de alta disponibilidad.

5.3.2.7 Capacidad del servidor de generar:

a) Mínimo 80 transacciones por segundo con llaves de 2048 bits

5.3.2.8 Funcionalidades:

a) Administración basada en web seguro (HTTPS) con requerimiento de certificado operador.
b) Capacidad ilimitada de generación de certificados sin coste adicional
c) Conectividad con bases de datos externas incluyendo PosgreSQL, Oracle y/o SQLServer,
d) Generación de certificados desde un dispositivo acreditado de forma segura
e) Generación de certificados por políticas preconfiguradas
f) Capacidad de publicar certificados y CRL en LDAP, Web.
g) Sincronización del reloj del sistema vía NTP
h) Notificación de errores automático
i) Capacidad de personalizar los menús de interface gráfica
j) Interfaz de usuario en español
k) Todos los documentos, paneles gráficos, interface de usuario y mensajes de error deberán estar en español.
l) Todos los elementos de la solución, aplicación, hardware, software y HSMs deben ser del mismo fabricante, para facilitar la responsabilidad sobre el proyecto y la resolución de las posibles incidencias. Capacidad de entregar los HSMs abiertos y que sean cerrados en presencia de los funcionarios

correspondientes, para garantizar que no se introduce ningún elemento externo que pueda ser considerado como inseguro por las autoridades pertinentes.

5.3.2.9 Otros:

a) Configuración previo levantamiento de información, configuración de los equipos en base a esa información recabada y elaboración de toda la documentación relativa a las políticas de certificación, que se acople a los procedimientos y políticas de la DIGERCIC.

5.3.3 Servidor de Autoridad de Certificación Subordinada

A continuación se presenta el tipo hardware (servidor) con HSM y aplicación específicas para la Autoridad de Certificación Subordinada.

5.3.3.1 Características Específicas

- Aplicación SW de AC subordinada basada en estándares abiertos
- Configuración como autoridad de certificación subordinada.

5.3.3.2 Algoritmos y Funciones Hash

- Similar al punto 5.3.2.3, literales a), b), c), d).

5.3.3.3 Cumplimiento de Estándares

- Similar al punto 5.3.2.4, literales a), b), c), d).

5.3.3.4 Certificaciones de seguridad:

- Similar al punto 5.3.2.5, literales a), b).

5.3.3.5 Alta disponibilidad.

- Similar al punto 5.3.2.6, literal a).

5.3.3.6 Capacidad del servidor de generar:

- Similar al punto 5.3.2.7, literal a).

5.3.3.7 Funcionalidades:

- Similar al punto 5.3.2.8, literales a), b), c), d), e), f), g), h), i), j).
- Capacidad de aceptar peticiones de varias autoridades de registro de forma simultánea.

- Comunicación segura entre AC subordinadas con la AC raíz y con las ARs, de HSM a HSM.

5.3.3.8 Otros:

Similar al punto 5.3.2.9, literal a).

5.3.4 Servidor de Autoridad de Registro

A continuación se presenta el tipo hardware (servidor) con HSM y aplicación específicas para la Autoridad de Registro.

5.3.4.1 Características Específicas

- Similar al punto 5.3.2.1 literales a), b), c), d), e), f), g).
- Aplicación SW Autoridad de Registro basada en estándares abiertos.
- Configuración como autoridad de registro.

5.3.4.2 Conectividad

Similar al punto 5.3.2.2 literales a), b), c).

5.3.4.3 Algoritmos y Funciones Hash

Similar al punto 5.3.2.3 literales a), b), c), d).

5.3.4.4 Cumplimiento de Estándares

Similar al punto 5.3.2.4 literales a), b), c), d).

5.3.4.5 Certificaciones de seguridad

Similar al punto 5.3.2.5 literales a), b).

5.3.4.6 Alta disponibilidad

Similar al punto 5.3.2.6 literal a).

5.3.4.7 Capacidad del servidor de generar

80 transacciones por segundo con llaves de 2048 bits.

5.3.4.8 Funcionalidades

- Similar al punto 5.3.2.8 literal a), b), c), g), h), i).
- Generación de claves desde un dispositivo acreditado de forma segura.
- Comunicación segura componentes.

- Capacidad de soportar ilimitado número de operadores.

5.3.4.9 Otros,

Similar al punto 5.3.2.9 literal a).

5.3.5 Servidor de Autoridad de Validación

A continuación se presenta el tipo hardware (servidor) con HSM y aplicación específica para el servidor de Autoridad de Validación

5.3.5.1 Características Específicas

- Similar al punto 5.3.2.1 literales a), b), c), d), e), f), g), h).
- Aplicación de Autoridad de Validación basada en estándares abiertos.
- La VA debe permitir conectarse a cualquier aplicación o aplicaciones sin ningún coste adicional por licenciamiento.

5.3.5.2 Conectividad

Similar al punto 5.3.2.2 literales a), b), c).

5.3.5.3 Algoritmos y Funciones Hash:

Similar al punto 5.3.2.3 literales a), b), c), d).

5.3.5.4 Cumplimiento de Estándares:

- Protocolo estándar OCSP (Online Certificate Status Protocol)
- NTP v3.0
- PKCS#1, PKCS#8, PKCS#10
- X.509v3 CRLv2 rfc3280
- RFC 2560
- HTTP, HTTPS

5.3.5.5 Certificaciones de seguridad

Similar al punto 5.3.2.5 literales a), b).

5.3.5.6 Alta disponibilidad

Similar al punto 5.3.2.6 literal a).

5.3.5.7 Capacidad del servidor de generar:

Similar al punto 5.3.2.7 literal a).

5.3.5.8 Funcionalidades:

- Generación de peticiones de certificados
- Acceso a información de revocación de base de datos de la Autoridad de Certificación y CRL en LDAP, Web.
- Sin costo de licencias referente al uso de servicio OCSP por número de usuarios
- Sincronización del reloj del sistema vía NTP
- Administración basada en web seguro (HTTPS) con requerimiento de certificado operador
- Acceso a usuarios finales a través de HTTP-HTTPS
- Acceso a base de datos externas.- PosgreSQL, Oracle y/o SQLServer
- Notificación de errores automático

5.3.5.9 Otros

Similar al punto 5.3.2.9 literal a).

5.3.6 Infraestructura de Clave Pública Firma Electrónica DIGECIC

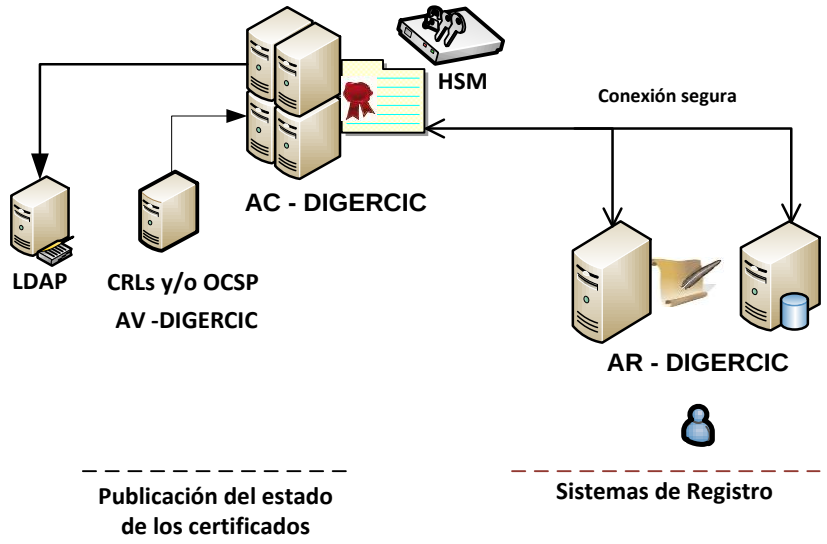


Figura 35. Esquema Autoridad de Certificación DIGERCIC

5.3.7 Servidor Autoridad de Sellado de Tiempo

A continuación se presenta el tipo hardware (servidor) con HSM y aplicación específica SW de la Autoridad de Sellado de Tiempo.

5.3.7.1 Características Específicas

- Similar al punto 5.3.2.1 literal a), b), c),d), e), f), g), h)
- Aplicación SW de TSA basada en estándares abiertos
- Hardware criptográfico certificado integrado.
- Configuración del servicio de sellado de tiempo.
- La TSA debe permitir conectarse a cualquier aplicación o aplicaciones sin ningún coste adicional por licenciamiento.

5.3.7.2 Conectividad

Similar al punto 5.3.2.2 literal a), b), c).

5.3.7.3 Algoritmos y Funciones Hash:

Similar al punto 5.3.2.3 literal a), b), c), d).

5.3.7.4 Cumplimiento de Estándares:

- Certificados X.509 v3
- PKIX Time stamp protocol (RFC3161)
- ETSI TS 102 023 y ETSI TS 101 861

5.3.7.5 Certificaciones de seguridad

Similar al punto 5.3.2.5 literales a), b).

5.3.7.6 Alta disponibilidad

Similar al punto 5.3.2.6 literales a).

5.3.7.7 Capacidad del servidor de generar:

80 time stamps por segundo con llaves de 2048 bits RSA.

5.3.7.8 Funcionalidades:

- Protocolo de sellado de tiempo HTTP siguiendo estándar RFC3161.
- APIs en . NET o JAVA
- Calibración automática del tiempo en servidores NTP.
- La selección de servidores NTP debe ser abierta y libre, pudiendo utilizarse seleccionar cualquier servidor disponible sin limitarse a un servidor NTP específico
- Solo podrán incluirse estándares abiertos sin estar permitidas versiones propietarias del protocolo NTP o cualquier otro
- Capacidad de configurar múltiples repositorios de fuentes de tiempo distribuidos en distintas zonas geográficas
- Administración del sistema vía HTTPS con requerimiento de certificado de operador
- Debe permitir la integración con un Máster Clock.
- Además de los literales c), h), j) del punto 5.3.2.8.

- Generación de peticiones de certificados desde un dispositivo acreditado de forma segura.

5.3.7.9 Otros:

- Similar al punto 5.3.2.9, literal a).

5.3.7.10 Esquema Infraestructura de Clave Pública Sellado de Tiempo TSA

La siguiente figura muestra la arquitectura general de la Autoridad de Certificación TSA y su interrelación con los componentes de red (mediante el protocolo de sellado de tiempo de IETF). TSA puede operar con un HSM (en red o interno) y requiere acceso tanto a una base de datos como a una fuente de tiempo en red (accesible por ejemplo mediante NTP).

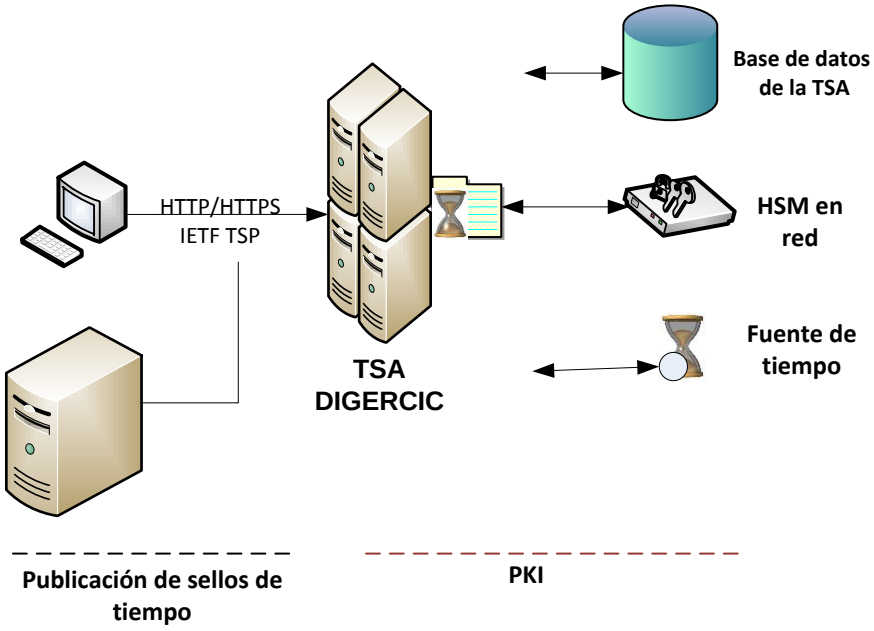


Figura 36. Esquema Autoridad de Sellado de Tiempo - TSA DIGERCIC

5.3.8 Servidor de Firma Electrónica

A continuación se presenta el tipo hardware (servidor) con HSM y aplicación SW específica de firma.

5.3.8.1 Características Específicas

- Similar al punto 5.3.2.1 literales a), b), c), d), e), f), g), h),

- Aplicación SW de firma en el apliance y basada en estándares abiertos.
- Capacidad ilimitada de firmas sin coste adicional.
- Capacidad de almacenar los certificados dentro del HSM sin costo adicional.
- Plataforma de administración de claves.
- El servidor de firma electrónica debe permitir conectarse a cualquier aplicación o aplicaciones sin ningún coste adicional por licenciamiento.

5.3.8.2 Conectividad

- Similar al punto 5.3.2.2 literales a), b), c).
- Interface CSP.

5.3.8.3 Algoritmos y Funciones Hash

Similar al punto 5.3.2.3 literales a), b), c), d).

5.3.8.4 Cumplimiento de Estándares:

- RSA PKCS#1_v1.5.
- RSA X509.

5.3.8.5 Certificaciones de seguridad

Similar al punto 5.3.2.5 literales a), b).

5.3.8.6 Alta disponibilidad

Similar al punto 5.3.2.6 literales a).

5.3.8.7 Capacidad del servidor de generar

- Mínimo 30 procesos de firma electrónica en PDF nativo por segundo con llaves de 2048 bits
- Mínimo 70 procesos de firma electrónica en PkCS 7 RSA por segundo con llaves de 2048 bits
- Mínimo 50 procesos de firma electrónica en XAdEs por segundo con llaves de 2048 bits

5.3.8.8 Funcionalidades

Además de los literales c, h, i, j, k, l del punto 5.3.2.8

- Firma para ilimitado número de documentos.
- Capacidad de firmar documentos en varios formatos: pdf, binarios, XadES, Pades, etc.

- Verificación de firma electrónica.
- Firma electrónica con soporte para sellado de tiempo
- Generación de peticiones de certificados desde un dispositivo acreditado de forma segura.
- Módulo CSP que garantizan la funcionalidad del dispositivo de firma en entornos Windows, Mac, Mozilla, Linux.
- Importa certificados hacia la placa criptográfica c),
- Administración basada en web seguro (HTTPS).
- Aplicación cliente para ejecución stand-alone e integración con aplicaciones Java o .Net.
- Soportar integración con máquinas escaneadoras para la firma instantánea de documentos escaneados antes de su incorporación al sistema de almacenamiento electrónico

5.3.8.9 Otros:

- Similar al punto 5.3.2.9, literal a).

5.4 TIPOS DE DISPOSITIVOS, SISTEMAS OPERATIVOS Y ESTÁNDARES PARA ACCESO AL CHIP DE LA TARJETA ELECTRÓNICA

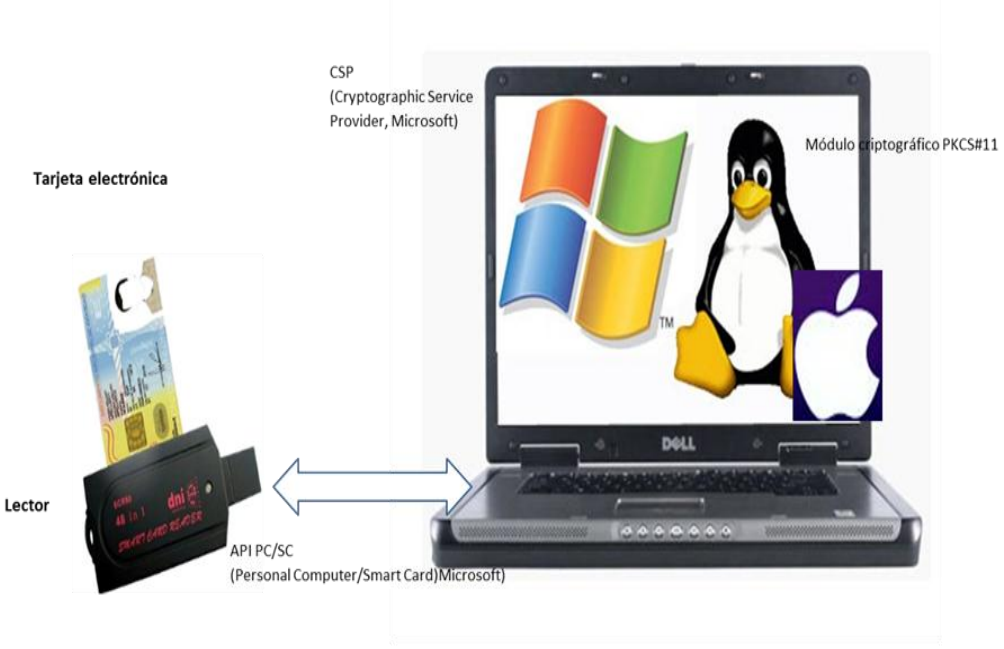


Figura 37. Acceso Tarjeta Electrónica

Fuente: (Lozano & Azcárate, 2010)

Para usar el DNI electrónico desde un computador será necesario disponer de un lector de tarjetas compatible con el DNIe.

El lector debe cumplir con mínimo:

- El estándar ISO 7816 (1, 2 y 3)
- Soportar tarjetas asíncronas basadas en protocolos T=0 y T=1
- Soportar velocidades de comunicación mínimas de 9.600 bps
- Soportar los estándares:
    - API PC/SC (Personal Computer/Smart Card)
    - CSP (Cryptographic Service Provider, Microsoft)
    - API PKCS#11

Además, para poder interaccionar adecuadamente con las tarjetas criptográficas (DNIe), el computador deberá tener instalados unas ‘piezas’ de software denominadas módulos criptográficos.

En un entorno Microsoft Windows, el equipo deberá tener instalado un servicio "CryptographicServiceProvider" (CSP).

En los entornos UNIX / Linux o MAC, se podrá utilizar el DNI electrónico a través de un módulo criptográfico PKCS#11 (Lozano & Azcárate, 2010).

5.5 ORGANIGRAMA ESTRUCTURAL DE LA UNIDAD DE NEGOCIOS DE CERTIFICACIÓN DIGITAL – UNCD DE LA DIGERCIC

Tomando en cuenta la visión de la DIGERCIC para los siguientes años se plantea crear una unidad de negocios de certificación digital bajo la Dirección de Servicios Electrónicos que estará conformada de la siguiente manera:

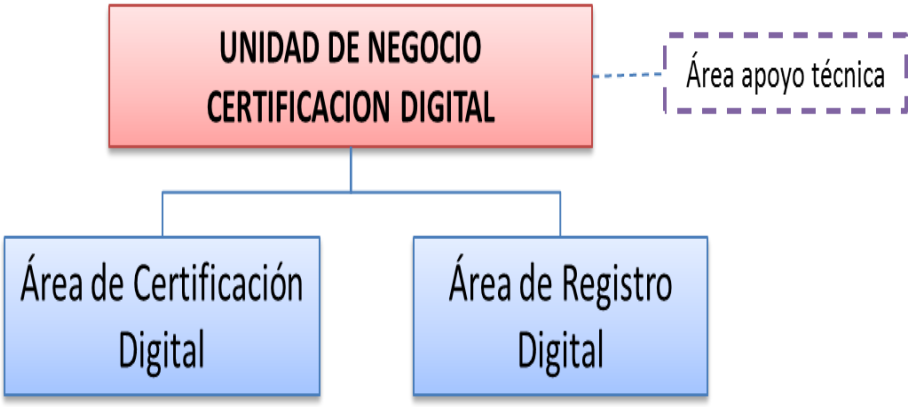


Figura 38. Organigrama de UNCD - DIGERCIC

La unidad de negocio de certificación digital será la encargada de la generación y la gestión del ciclo de vida de los certificados digitales para las personas naturales y jurídicas.

5.5.1 Flujograma del proceso de Certificación Digital

Para una mejor compresión de las actividades que realizará la DIGERCIC, se presenta a continuación el flujograma del proceso de Certificación Digital.

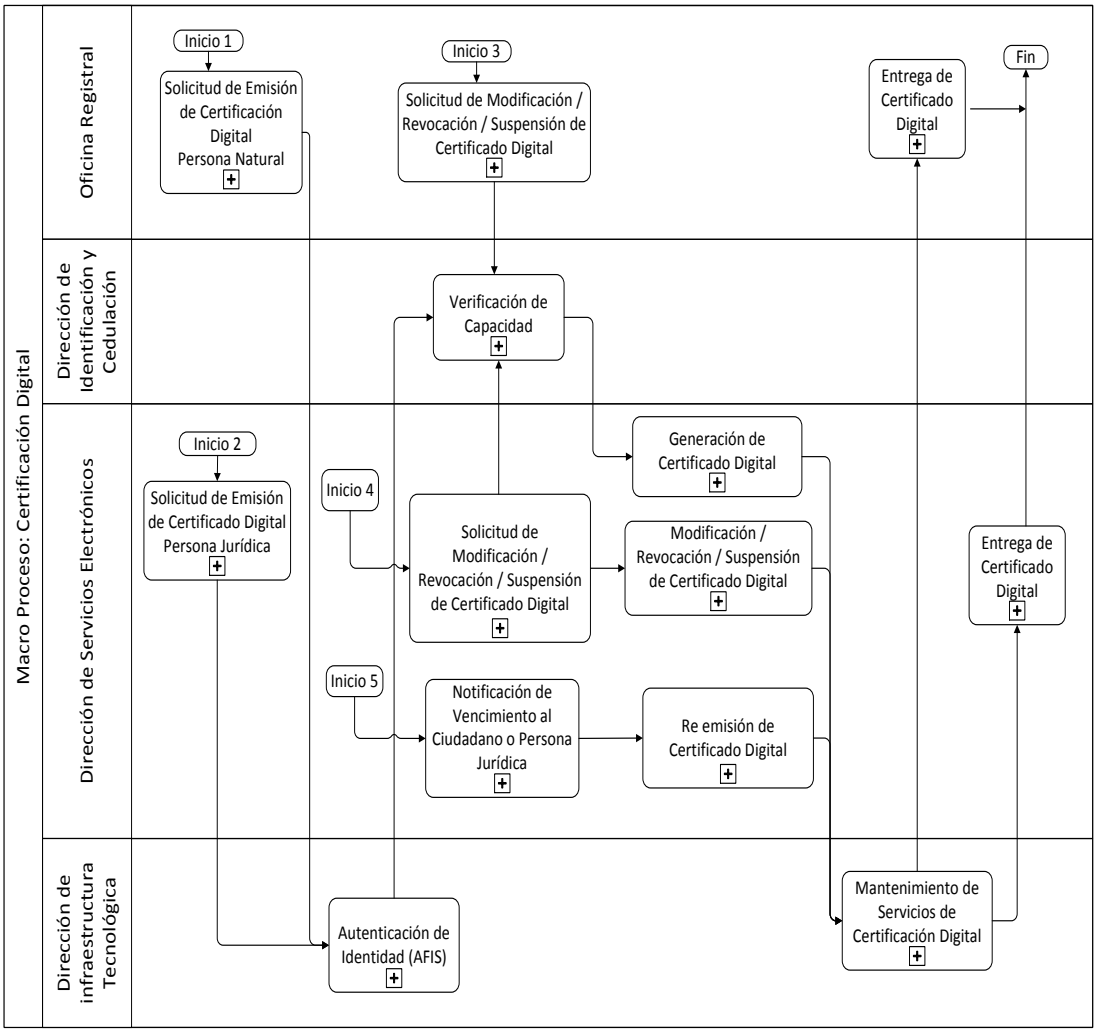


Figura 39. Flujograma del proceso de Certificación Digital

Fuente: (RENIEC, sf)

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

La infraestructura actual de la DIGERCIC no es suficiente para brindar el servicio de firma electrónica, requiere implementar una infraestructura de clave pública en base a las normas y estándares actuales.

Como resultado del análisis del nivel de cumplimiento de la Norma ISO 27001:2005 Sistema de Información de Gestión de la Seguridad por parte de la DIGERCIC se ha determinado que las áreas de control de la norma que presentan un menor nivel de cumplimiento son: Políticas de Seguridad, Gestión de Activos, Gestión de Incidentes de Seguridad de la Información, Gestión de la Continuidad del Negocio.

De la evaluación activa de las medidas de seguridad de los sistemas de la DIGERCIC mediante test de penetración se obtuvo que los servidores presentan solo vulnerabilidades de bajo factor de riesgo.

Se efectuaron pruebas exitosas de lectura de parámetros encriptados de la cédula de ciudadanía mediante el uso de una herramienta personalizada de prueba para desarrollo de software (Software Development Kit o SDK) y un chip Secured Access Module (SAM).

Con la evaluación del cumplimiento de los requisitos técnicos del Sistema Magna y de la DIGERCIC para entidades de certificación de acuerdo con la "Guía de Acreditación de Entidades de Certificación EC Versión 3.3"; se determina que el sistema Magna y la DIGERCIC están en capacidad técnica de soportar el servicio de firma electrónica.

De la evaluación de las seguridades de la información de las tarjetas de identificación se determina que el chip de la cédula cumple con el nivel EAL 5 + EAL4+ de Evaluación de la Garantía de Seguridad de acuerdo con la norma ISO/IEC 15408 Common Criteria donde el desarrollador del chip alcanza la máxima garantía de ingeniería de seguridad positiva mediante la aplicación moderada de técnicas de

ingeniería de seguridad y asegura la resistencia relativa a los ataques de penetración al chip de la cédula.

El hardware del chip soporta la infraestructura de los algoritmos de clave pública/privada, las recomendaciones de los tamaños mínimos de claves de firma electrónica para Entidades de Certificación, llaves firmantes del documento y claves de autenticación. La integridad, autenticidad y confidencialidad de los datos almacenados digitalmente están de acuerdo con la OACI NTWG, PKI para los documentos de viaje de lectura mecánica conforme ICC Lectura (solo acceso).

El sistema operativo del chip es capaz de respaldar futuros segmentos de memoria que no sean de la OACI (dirigidos a la aplicación individual de IDs - AID) para fines especiales como aplicaciones de ePKI, X.509, RSA (PKCS#1), perfil (PKCS#15), soporte a CWA 14890 -1, -2; autenticación (interna y externa) conforme a ISO 17816 -4 y -8; estándar de Firma Digital (DSS) FIPS 186-2.

La cédula electrónica a futuro permitirá ser usado para servicios de firma electrónica, esto permitirá identificar a los ciudadanos no solo en el mundo físico (funcionalidad actual), sino en el mundo de los servicios informáticos (futura funcionalidad). Esta capacidad permitirá que el eDNI se convierta en el generador de facilidades para viabilizar el Comercio y Gobierno electrónico en el Ecuador.

6.2 RECOMENDACIONES

Se recomienda crear un modelo jerárquico de Infraestructura de Firma Electrónica para la República del Ecuador siendo de aplicación para las Entidades de Certificación de Información y Servicios Relacionados tanto por el sector público como el privado.

Reforma de la normativa sobre comercio electrónico y firma electrónica con el fin de reordenar y racionalizar los recursos en materia de infraestructura de firma electrónica a nivel nacional donde sea considerada la ARCOTEL como Entidad de Acreditación y Control de Certificación Electrónica (EACCE) y la creación de una Autoridad de Certificación Raíz del Ecuador (ACREC).

La DIGERCIC para brindar el servicio de firma electrónica debe desarrollar e implantar un plan a largo plazo para una infraestructura de clave pública (PKI) en el

que se debe considerar lo siguiente: implantar un sistema de gestión de calidad para los servicios de firma electrónica, implantar un sistema de gestión de la seguridad de la información basada en la norma ISO 27001, y de manera especial el desarrollo de APIs para acceso a datos del chip de la cédula.

La DIGERCIC deberá establecer el marco legal y el modelo operativo (declaraciones de prácticas y políticas de certificación) a través del cual el ciudadano accederá o hará uso de estos servicios electrónicos. Las declaraciones de prácticas y políticas de certificación se deben definir y aplicar para todos los participantes relacionados con el uso de la cedula electrónica, como son las Autoridades de Certificación, Autoridades de Registro, Ciudadanos y Terceros Vinculados, entre otros.

Debido a la considerable diferencia en los periodos de validez de las claves y certificados de la PKI para el servicio de firma electrónica y el servicio de pasaportes electrónicos la DIGERCIC deberá realizar un nuevo proyecto independiente al desarrollado en este trabajo para implementar una infraestructura de clave pública que permita ofrecer el servicio de pasaportes electrónicos.

BIBLIOGRAFIA

INE Instituto Nacional de Estadísticas. (2010). *Estadísticas de certificado de firma electrónica DNIe de España.*

AGESIC, Agencia de gobierno electrónico y sociedad de la informacion. (s.f.). Obtenido de www.cert.uy/wps/wcm/connect/1de4ea8

ANGELBORROY. (18 de 7 de 2012). Recuperado el 21 de 9 de 2013, de http://angelborroy.wordpress.com/2012/07/18/estadisticas-de-uso-real-del-dni-electronico-en-espana

Cuervo, J. (sf). *Firma Digital y Entidades de Certificación.* Recuperado el 5 de 10 de 2013, de http://www.informatica-juridica.com/trabajos/firma_digital.asp

CYBSEC Security Systems. (2009). Seguridad en Redes de Telecomunicaciones. *Criptografía*.

Dirección General de Registro Civil, Identificación y Cedulación. (2010). *Informe No. 11: Plan de Sociabilización y Usabilidad del nuevo DIN.*

Dirección General de Registro Civil, Identificación y Cedulación. (2013). *Actualización del Proyecto:Modernización del Sistema Nacional de Registro Civil, Identificación y Cedulación - Fase Masificación.*

Dirección General de Registro Civil, Identificación y Cedulación. (2013). *Reporte Indicadores GPR- DIGERCIC agosto de 2013.*

Estepa, R. (2004). *Transmisión y Digitalización.*

http://angelborroy.wordpress.com/2012/07/18/estadisticas-de-uso-real-del-dni-electronico-en-espana. (s.f.). Recuperado el 21 de 9 de 2013

INDECOPI, Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual. (2007). Recuperado el 3 de 6 de 2013, de http://www.indecopi.gob.pe/repositorioaps/0/6/jer/fd_guiasacredcdec/Gu%C3%ADaAcredEC.pdf

INEI. (s.f.). *Infraestructura de Llave Pública para el Estado Peruano (PKI) Framework.* Recuperado el 25 de 9 de 2013, de http://www.inei.gob.pe/web/info_proy/attach/4821.pdf

KRAFFT, R. (2002). *LA FIRMA ELECTRÓNICA Y LAS ENTIDADES DE CERTIFICACIÓN.*

Ley de Comercio Electrónico, Mesaje de Datos y Firma Eléctrónica. (2002).

López, M. (2012). *Los Sistemas de Información: Evolución y Desarrollo.*

Lucena López, M. J. (2007). *Criptografía y Seguridad en Computadores* (4 ed.).

Martínez, S. (2005). *Diseño e Implementación de una Autoridad Certificadora en Plataformas Móviles.* (I. T. MONTERREY, Ed.) México D.F.

MathCon. (sf). Obtenido de http://www.math.com.mx/criptografia.html

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2011). *Control de Asistencia en base a la Cédula Electrónica de Identidad.*

Moneda, F. N.-R. (sf). Recuperado el 27 de 11 de 2014, de http://portalae.sci.uma.es:8080/export/sites/default/uma/documentos/criptografia_certificado_digital_firma_digital.pdf

OACI Organización de Aviación Civil Intenacional. (2008). Doc 9303 - Documento de viaje de lectura mecánica.

ONGEI, Oficina Nacional de Gobierno Electrónico e Informatica. (2002). *Peru Gobierno Electrónico.* Recuperado el 25 de 9 de 2013, de http://www.ongei.gob.pe/publica/proyectos/4821.pdf

Organización de Aviación Civil Internacional- OACI. (2008). Doc 9303.

OTI - ON TRACK INNOVATIONS LTD. (2013). Recuperado el 3 de 12 de 2013, de http://84.95.244.105/Magna

Peña, A. (2006). *Ingeniería de Software:Una Guía para Crear Sistemas de Información.*

Sistema Económico Latinoamericano y del Caribe SELA. (2012). *Fundamentos de la firma digital y su estado del arte en América Latina y el Caribe.* Caracas.

TOMAS, & FRANCISCO, V. (1996). *El orden Jurídico Medieval.* Madrid, : Marcial Pons.

ABREVIATURAS Y ACRÓNIMOS

TÉRMINO	DESCRIPCIÓN
AC	Autoridades de Certificación
AES	Advanced Encryption Standard
AFIS	Automated Fingerprint Identification System
ANSI	American National Standards Institute
API	Interfaz de Programación de Aplicaciones
AR	Autoridad de Registro
ARCOTEL	Agencia de Regulación y Control de Telecomunicaciones
AV	Autoridad de Validación
BAC	Control de Acceso Básico
C	Country (País). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
CDPs	CRL Distribution Point
CN	Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
CONATEL	Concejo Nacional de Telecomunicaciones
CP	Políticas de Certificados
CPS	Declaración de Prácticas de Certificación
CRLs	Listas de revocación de certificados
CSCA	Autoridad de Certificación de firma de país
CSP	Proveedor de Servicios Criptográficos
DES	Data Encryption Standard
DIGERCIC	Dirección General de Registro Civil identificación y Cedulación
DN	Nombre Distintivo, son los campos que sirven para identificar a un certificado digital, que además es único.
DN	Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de la estructura de directorio X.500.
DN	Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de la estructura de directorio X.500.
DNI	Documentos de Identificación Nacional
DNIe	Documento Nacional de Identificación electrónico.
DS	Documento Firmante
EAC	Extended Access Control
EC	Entidades de Certificación
ECDSA	Elliptic Curve Digital Signature Algorithm
ECN	Entidad de Certificación Nacional
eGOV	Gobierno Electrónico
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard (Estándares del Gobierno Norteamericano para el procesamiento de la información)
FODA	Fortalezas, Oportunidades, Debilidades y Amenazas

FTP	File Transfer Protocol / Protocolo de Transferencia de Archivos
HSM	Hardware Security Module / Módulos de Seguridad de Hardware
HTTP	Hypertext Transfer Protocol / Protocolo de transferencia de hipertexto
HTTPS	Hypertext Transfer Protocol Secure / Protocolo seguro de transferencia de hipertexto
ICAO	International Civil Aviation Organization
IDEA	International Data Encryption Algorithm
IEC	Comisión Electrotécnica Internacional
INDECOPI	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual
ISO	Organización Internacional de Normalización
ISO	Organización Internacional de Normalización
ITU	Unión Internacional de Telecomunciaciones
L	Localidad. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
LACNIC	Registros de Direcciones de Internet para Latinoamérica y el Caribe
LDAP	Lightweight Directory Access Protocol
LDS	Logical Data Structure
MAGNA	Plataforma de software personalizable para el registro de la población basada en la Web y la producción, emisión de documentos de identificación nacional como DNI, pasaporte electrónico, Visa.
MINTEL	Ministerio de Telecomunicaciones y de la Sociedad de la Información
MoC	Math on Card
MTBF	Tiempo medio de fallas
NTP	Network Time Protocol
O	Organization. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
OACI	Organización de Aviación Civil Internacional
OCSP	Online Certificate Status Protocol
OID	Object identifier (Identificador de objeto único)
OID	Object identifier (Identificador de objeto único)
OMSC	Observatorio Metropolitano de Seguridad Ciudadana
OU	Organizational Unit. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
OU	Organizational Unit. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards. Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente.
PKCS	Public-Key Cryptography Standards
PKI	Infraestructura de Clave Pública
RFC	Request For Comments (Estándar emitido por la IETF)
RFID	Tecnología de Radio Frecuencia
RSA	Rivest, Shamir y Adleman

SAM	Secure Access Module
SDK	Software Development Kit
SENATEL	Secretaria Nacional de Telecomunicaciones
SHA	Secure Hash Algorithm / Algoritmo de Hash Seguro
SN	surName (apellido). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
SSL	Secure Sockets Layer / Capa de conexión segura
SW	Sotware
TLS	Transport Layer Security / Seguridad de la capa de transporte
TSA	Autoridades de Sello de Tiempo
UNCD	Unidad de Negocios de Certificación Digital
UTF8	Unicode Transformation Format - 8 bits
VPN	Red Privada Virtual
X.500	Conjunto de estándares de redes de ordenadores de la ITU-T sobre servicios de directorio
X.509	Especifica formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación.

ANEXO A

Encuesta cumplimiento de la norma ISO 27001:2005 Sistema de Información de Gestión de la Seguridad 11 áreas de control.