INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 64-77 https://doi.org/10.33936/isrtic.v4i1.2348 | ISSN 2550-6730

Recibido: 02/04/2020
Aceptado: 12/05/2020

Estudio exploratorio de la seguridad del DNI electrónico para su aplicación en Ecuador

Cristhian Cedeño Sarmiento [1] Francisco Bolaños Burgos [1] Alex Gregorio Mendoza Arteaga [1] Wilton Rafael Saltos Rivas [2]

[1]Universidad Espíritu Santo – Ecuador.
[1]Universidad Técnica de Manabí – Ecuador

cfcedeno@uees.edu.ec, fcobolanos@uees.edu.ec, alexmendoza@uees.edu.ec, w.saltos@utm.edu.ec

RESUMEN
En la actualidad la necesidad de contar con un dispositivo de identificación electrónica seguro que permita identificar y autenticar a los ciudadanos en actividades en línea es primordial, más aún en países que se encuentran implementando políticas de gobierno electrónico en su población y ante eventos diarios de ataques de suplantación de identidad en línea. En el presente artículo de revisión se realiza un análisis de la seguridad que existe en la implementación del documento nacional de identificación electrónico (DNIe) en España, las versiones que ha tenido el dispositivo, la tecnología que posee en la actualidad, la estructura interna, los tipos de certificados digitales de seguridad que almacena el chip criptográfico, la infraestructura de clave pública que soporta su funcionamiento y los casos de usos que se han propuesto para el dispositivo. Adicional se incluye una revisión de países que implementan dispositivos de identificación electrónica en ambientes de gobierno electrónico para sus ciudadanos, las posibles debilidades presentadas en este tipo de tarjetas criptográficas así como las contramedidas definidas por autores reconocidos en ambientes de ataques de canal lateral, por último se presenta una revisión de las instituciones públicas y privadas existentes en Ecuador que podrían aportar en un futuro proceso de implementación del nuevo dispositivo de identificación digital en el país.
Palabras-clave: DNIe, Identificación electrónica, gobierno electrónico, Ecuador.

ABSTRACT
At present, the need for a secure electronic identification device to identify y authenticate citizens in online activities is paramount, even more so in countries that are implementing e-government policies in their population y in the face of daily attacks Online spoofing. In this review article, an analysis is made of the security that exists in the implementation of the national electronic identification document (DNIe) in Spain, the versions that the device has had, the technology it currently has, the internal structure, The types of digital security certificates that the cryptographic chip stores, the public key infrastructure that supports its operation, y the proposed use cases for the device. Additional includes a review of countries that implement electronic identification devices in e-government environments for their citizens, the possible weaknesses presented in this type of cryptographic cards as well as the countermeasures defined by recognized authors in environments of lateral channel attacks, lastly A review of public y private institutions in Ecuador that could contribute to a future process of implementation of the new digital identification device in the country is presented.
KEYWORDS: DNIe; electronic identification; e-government; Ecuador

1. Introducción

Se vive uno de los tiempos más conflictivos en la lucha por mantener la privacidad en los datos, con cibercriminales acechando por doquier, haciendo uso de la tecnología para realizar análisis minuciosos de vulnerabilidades y encontrar fallos en dispositivos de seguridad calificados como seguros [1], en una sociedad en donde las personas se encuentran registradas en miles de bases de datos dispersas, haciendo uso de múltiples identidades en la red [2], existiendo inclusive restricciones mínimas e insuficiente protección a los menores de edad al momento de acceder a internet convirtiéndolos en entes vulnerables a actividades delictivas como abusos, pedofilia, suplantación de identidad, etc. [3]

La suplantación de identidad, el robo de datos y el acceso fraudulento en los sistemas de información ocurren con frecuencia, el objetivo de los atacantes es espiar y robar información confidencial de sus víctimas, así lo demuestra la empresa[4] la cual detectó un promedio de 45 diferentes ataques por segundo en América Latina en un periodo comprendido entre julio 2018 a julio 2019.

Por otra parte, [5] exponen que cuando existe una suplantación de identidad, es difícil poder distinguir al verdadero titular del impostor, y ésta suplantación, en el mayor de los casos es detectada después de haberse consumado un delito, cuando el titular de la información se encuentra involucrado en actos ilícitos o incluso cuando se ha tenido una afectación económica producto de transacciones electrónicas no autorizadas. Ya en el año 1987 [6] proponían las primeras debilidades al no usar tecnología de identificación digital, entre ellas: fotocopias de pasaportes por gobiernos discrepantes, números de tarjeta de crédito clonados y contraseñas vulnerables a hackers y grabaciones.

De la misma forma [7] coinciden en que uno de los retos generados por el rápido desarrollo de las tecnologías de la información es brindar y garantizar a los ciudadanos de mecanismos que aseguren la privacidad de su información. En el mismo sentido [8] señalan que es necesario implementar mecanismos de seguridad que permitan al común de los ciudadanos mantener su información personal íntegra, confidencial y segura, para con ésta confianza adquirida realizar transacciones electrónicas autorizadas y sentirse seguros que la información transmitida viaja por canales electrónicos confiables.

Para verificar la identidad de una persona y garantizar la privacidad en el acceso a los datos [9] exponen cuatros métodos distintos para hacerlo: conociendo una secuencia de seguridad (contraseña), portando un documento o carnet de identificación (medio físico), mediante la verificación de características propias del usuario (biometría) y por último verificando la posición geográfica de un usuario (georeferenciación). [5] concuerdan en que debe existir un equilibrio entre los mecanismos de seguridad para que, multiplicando los controles de acceso el fraude electrónico sea dificultoso y se minimice el acceso no autorizado a información privada, sin embargo partiendo de la premisa de que ningún sistema de seguridad es infalible, la recomendación sería entonces implementar sistemas de autenticación difíciles de violentar para que de esta manera el esfuerzo requerido en violentar el mismo sea superior a los beneficios obtenidos.

El mecanismo de seguridad que mayor expansión ha tenido hasta la actualidad es la contraseña, la cual se basa en el conocimiento que tiene un usuario sobre un conjunto de caracteres para autenticarse, y es debido a las vulnerabilidades y problemas generados en la implementación de autenticación por medio de contraseñas que surge la necesidad de implementar un segundo factor de autenticación utilizando por ejemplo un documento o carnet de identificación el cual permite autenticarse ante una persona o ante un dispositivo electrónico por medio de una serie de operaciones matemáticas tan complejas de forma que vulnerar la autenticación del usuario utilizando este segundo mecanismo sea una tarea realmente dificultosa [9].

Teniendo en cuenta que la validación de la identidad de una persona por medio de un carnet de identificación siempre se realizará de manera física, es preciso establecer procedimientos electrónicos para poder verificarla según los avances actuales de la tecnología. Es aquí donde surge el Documento Nacional de Identidad Electrónico (DNIe), el cual nace de la necesidad de otorgar identidad personal a los ciudadanos para acceder a servicios electrónicos acorde a los avances de la sociedad de la información (Ministerio del Interior - Gobierno de España, 2015).

Según lo indicado por [7][10], España es uno de los países pioneros a nivel mundial en la implementación de la tecnología del DNIe. En el Ecuador, tal como lo indica la Dirección General de Registro Civil, Identificación y Cedulación (2013), desde hace unos cinco años atrás se han desarrollado proyectos de

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 64-77 https://doi.org/10.33936/isrtic.v4i1.2348 | ISSN 2550-6730

actualización de la cédula de identidad, augurando la futura implementación de un estándar de identidad electrónica en el país, por lo cual el objetivo del presente estudio se centra en analizar la seguridad que brinda el dispositivo DNIe en los países donde se ha implementado, para de esta manera tener un punto de vista más amplio hacia su futura aplicación en el Ecuador, se detallan los usos propuestos por diferentes autores para el DNIe y una revisión de las instituciones que podrían aportar en un futuro proceso de implementación del dispositivo en el Ecuador.

2. Marco Teórico

DNIe

[10][11][12] exponen al DNIe como el documento que permite legitimar a su titular como auténtico y justifica de forma física y digital su identidad, así como la firma electrónica de documentos digitales, la unión de las medidas de acceso físico y las digitales ofrecen un nivel de protección alto permitiendo al usuario tener un dispositivo de autenticación prácticamente inviolable o falsificable. Este documento está formado sobre un soporte de policarbonato cuyo tiempo de duración se estima en 10 años como mínimo con un tamaño similar al de una tarjeta de crédito coincidiendo con lo indicado por [13] quien clasifica al DNIe como una tarjetas criptográficas dentro del grupo de tarjetas inteligentes, en la cual se pueden almacenar certificados digitales de seguridad de forma segura con la finalidad de firmar documentos o autenticarse sin necesidad que el certificado salga de la tarjeta gracias al uso del procesador criptográfico contenido en ella quien es el que realiza el proceso de la firma digital.

Versiones del DNIe

[10] indica que el DNIe en España se puso en marcha el 16 de marzo de 2006 siendo esta la primera versión del dispositivo en implementarse en dicho país. La versión vigente del DNIe en dicho país es la 3.0 la cual empezó a ser emitida a partir de enero del 2015. En dicha versión se incorpora la tecnología "Dual Interface" la cual permite conexión por medio de contactos o de forma inalámbrica mediante un emisor de frecuencia Near Field Communication (NFC). La interfaz con contactos permite mantener la compatibilidad del dispositivo con tecnologías anteriores, mientras que la conexión por radiofrecuencia permite leer el dispositivo mediante tecnología NFC (Ministerio del Interior - Gobierno de España, 2016). El objetivo de la versión 3.0 según lo explican [3] es facilitar su uso con teléfonos inteligentes evitando la limitante de acceso a lectores de tarjetas inteligentes por parte de los usuarios finales. En la figura 1 se detallan las características físicas del DNIe 3.0.

Near Field Communication (NFC)

[14] exponen que la tecnología de Comunicación de Campo Cercano por sus siglas en inglés NFC permite la conectividad entre dispositivos a una distancia máxima de 20 cm, la cual en la actualidad está siendo implementada por fabricantes de telefonía móvil y entidades bancarias para permitir al usuario final acceder a servicios electrónicos de una manera ágil y rápida.

Y es justamente mediante el estudio realizado por [15] en donde se propone la metodología utilizada para la autenticación mediante el DNIe a través de tecnología NFC, permitiendo el intercambio de información crucial por medio de comunicaciones inalámbricas seguras entre pares.

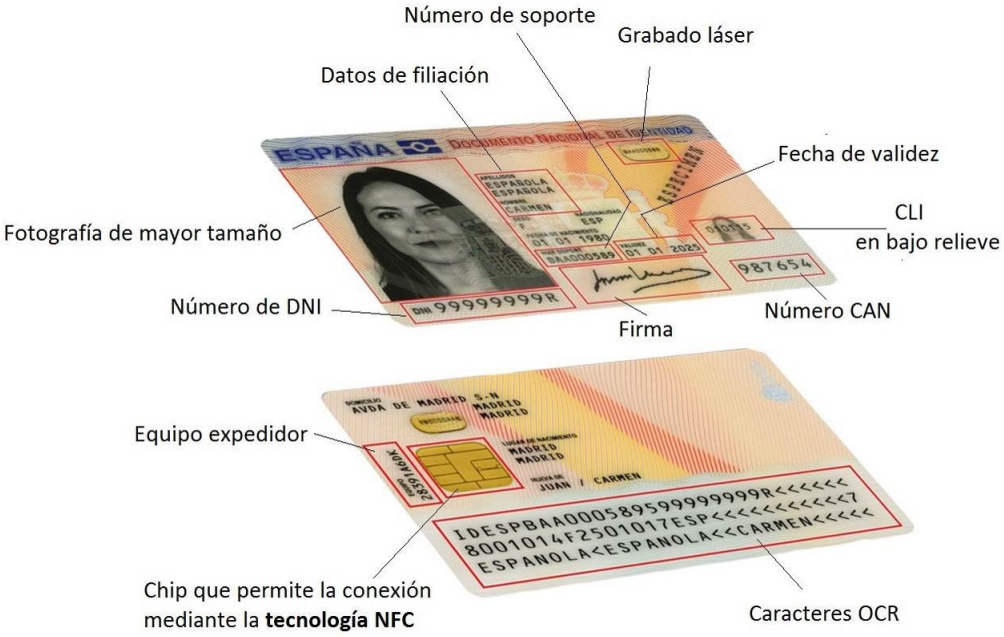

Figura 1: Descripción del DNI 3.0.
Fuente: (Ministerio del Interior - España, 2016)

Componentes y estructura interna del DNIe

El DNIe contiene los datos de filiación del ciudadano, la información biométrica (modelo dactilar, foto y firma manuscrita), y dos pares de claves RSA con sus correspondientes certificados de seguridad para autenticación y firma electrónica (Ministerio del Interior - Gobierno deEspaña, 2015). La información almacenada en el chip criptográfico se encuentra dividida en tres áreas con distintos niveles de acceso y condiciones de seguridad según lo descrito por [12][16][3]
Un área publica con acceso de solo lectura sin restricciones que contiene tres certificados x.509:

1. Certificado de seguridad único por cada DNIe el cual está asociado a la tarjeta inteligente con una clave pública RSA de 1024 bits.
2. Certificado de seguridad de la Autoridad de Certificación (CA), con una clave pública RSA de 1024 bits.
3. Certificado de la CA intermedia de la Dirección General de Policía, con una clave pública RSA de 2048 bits.

La segunda área del chip es privada con acceso de solo lectura posterior a la validación del código PIN del ciudadano (Personal Identification Number), esta sección contiene un certificado de seguridad para firma electrónica y un certificado de autenticación de usuario ambos una clave pública RSA de 2048 bits. La tercera área es de seguridad y con acceso de solo de lectura posterior a la verificación biométrica, esta acción solo es accesible desde los dispositivos biométricos ubicados en las oficinas de emisión de DNIe. Esta sección contiene los datos de filiación ciudadana (nombre, apellidos, fecha de nacimiento, etc.), una imagen digitalizada de la firma manuscrita del ciudadano y una fotografía del ciudadano.
De acuerdo a la estructura que posee el dispositivo de identificación electrónica antes descrito y por los niveles de seguridad establecidos en el chip, se desprende que detrás de la existencia del DNIe existe una

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 64-77 https://doi.org/10.33936/isrtic.v4i1.2348 | ISSN 2550-6730

infraestructura de clave pública (PKI) que soporta su funcionamiento y validación en España según lo descrito por [7].

Infraestructura de Clave Pública (PKI)

La PKI por sus siglas en inglés, tal como lo describe [7] es un conjunto de normas, procedimientos, software y personas, las cuales permiten la generación de certificados digitales de seguridad, mismos que tienen un tiempo de vigencia establecido de acuerdo a las normas legales de cada país y su funcionamiento se sustenta en la criptografía de clave pública desarrollada por [17], la PKI respalda el uso de la criptografía de clave pública según lo descrito por [18] puesto en este esquema la clave pública se almacena en un tercera entidad de confianza que valida la originalidad de la identidad del firmante.

El concepto de PKI, tal como indican [19] se ha afianzado a través de los últimos años usándose como referencia en la implementación de la nueva generación de aplicaciones haciendo posible el acceso a servicios de seguridad a gran escala inclusive en sistemas abiertos como la Internet.

La PKI según lo expone [20] forma parte del modelo de certificación TPT - Tercera Parte de Confianza o Trusted Third Party por sus siglas en inglés, la cual según lo indicado por [21] es el tercer nivel de seguridad en donde los fraudes de la autoridad de certificación deben ser detectables, en donde la autoridad de certificación no puede calcular las claves secretas de los usuarios y por medio de ésta entidad se puede comprobar la autenticidad de los certificados de seguridad electrónicos emitidos. Una PKI está formada por los siguientes componentes funcionales descritos por [13]: La Autoridad de Certificación (Certification Authority - CA), la autoridad de registro (Registration Authority - RA), la autoridad de Validación (Validation Authority - VA), la autoridad de sellado de tiempo (Time Stamping Authority - TSA). En la figura 2 se describe el modelo de referencia de la infraestructura de clave pública sobre la que funciona el DNIe en España en donde el proceso de pre personalización lo lleva a cabo la Fábrica Nacional de Moneda y Timbre y el proceso de expedición lo realiza el Ministerio del Interior mediante el organismo afiliado de la Dirección General de la Policía en calidad de Autoridad de Certificación Raíz.

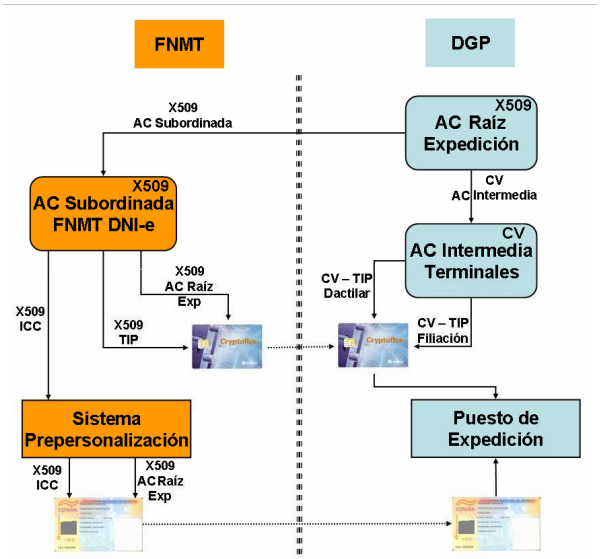

Figura 2: Modelo de referencia de proceso de pre personalización y expedición del DNIe
Fuente: (Crespo et al., 2006)

Los certificados digitales de seguridad que incorpora el DNIe cumplen con la función de confirmar que la clave criptográfica pública pertenece realmente a una persona determinada ayudando a evitar la suplantación de identidad, éstos certificados se componen de una clave pública, el nombre del titular, fecha de vencimiento, nombre de la autoridad de certificación, número de serie del certificado, y la firma digital del que otorga el certificado de seguridad según lo descrito por [22].

Las operaciones criptográficas de cifrado y descifrado que requieren el uso de una de las claves privadas almacenadas en el DNIe son ejecutadas por el chip interno, desempeñándose éste como una caja de seguridad digital para las claves privadas y como un coprocesador de operaciones criptográficas siempre y cuando se le suministre el PIN de usuario como método de autenticación [13].
Las áreas de uso del dispositivo DNIe incluyen transacciones comerciales, bancarias y servicios públicos. A continuación, se detallan algunos de ellos.
Usos del DNIe Las declaraciones de impuestos, el acceso a servicios de seguridad social, consulta de saldos de puntos de licencias de conducir, firma de contratos, registro de visitantes, transacciones financieras seguras en sistemas de administración público y privados son ejemplo de las áreas en donde se puede implementar el dispositivo ([11][13]).
En una investigación realizada por [23] se expone la futura utilización del DNIe como elemento para la autenticación de identidad del votante en un proceso de sufragio electrónico partiendo desde la autorización para realizar el voto hasta el proceso de la verificación individual de los resultados de la votación coincidiendo con lo propuesto por [24] quienes proponen la creación de una plataforma de sufragio seguro a través de Internet la cual permitiría recopilar firmas y soportar múltiples contextos mediante certificados digitales pudiendo ser utilizada dicha plataforma en votaciones de asambleas de accionistas, elección de dignidades populares, recolección de firmas de nominaciones, elecciones en reuniones de padres de familia en escuelas y colegios, entre las infinitas posibilidades de implementación del DNIe.
La posibilidad de implementar un sistema de control de transporte mediante GPS y autenticación vía DNIe para evitar vulnerabilidades relacionadas con suplantaciones de identidad en los conductores propuesta por [25], así como la metodología para autenticación en servicios de voz sobre IP mediante el dispositivo DNIe planteada por [26] son asimismo propuestas interesantes.
El sector de la salud también tiene un ejemplo de aplicación del DNIe mediante la propuesta de [27] en el cual presentan un caso real de éxito que permitió resolver incidentes relacionados con la privacidad de la información de los pacientes de un hospital en cumplimiento de la Ley Orgánica de Protección de Datos.
De forma adicional [3] presentan un uso muy particular del DNIe para realizar discriminaciones en cuanto a accesos de menores de edad en sitios web de adultos, es posible evitar suplantaciones de adultos haciéndose pasar como menores utilizando una validación de acceso a los sitios web mediante la fecha de nacimiento almacenada en el chip criptográfico del DNIe.
En el mismo sentido [28] realizaron una comparación entre el DNIe y una tarjeta inteligente para firmar prescripciones médicas, obteniéndose como resultado que el DNIe sobrepasa las funcionalidades de otras tarjetas de autenticación, pudiendo reemplazar a las mismas disminuyendo de esta forma los costos en la adquisición de dispositivos similares, unificando procesos y aprovechando la conectividad con tabletas y teléfonos inteligentes que el DNIe permite por medio de la tecnología NFC.
[29] proponen el uso del DNIe como testigo digital en procesos de evidencias electrónicas para escenarios de Internet de las cosas conectando el DNIe a través de una de sus interfaces (contactos o NFC) para firmar las evidencias directamente y obteniendo un código con validez legal asociado a la identidad del custodio de la evidencia facilitando su uso ante un tribunal de justicia sin tener que involucrar a terceras partes.
Con las demostraciones planteadas en las áreas antes mencionadas se visualiza que la implementación del DNIe genera un impulso en el aumento de transacciones comerciales electrónicas públicas y privadas haciendo que sea posible el desarrollo del gobierno electrónico (e-goverment) también denominado e-administración [10].
Gobierno electrónico [30] expresan que la interacción entre los ciudadanos con las administraciones gubernamentales a lo largo de los años ha sido una tarea compleja debido a las limitantes de horarios de oficina y largos tiempos de espera, coincidiendo con lo expuesto por [11] quienes plantean que el acceso a los servicios electrónicos debería estar disponible las 24 horas del día, siete días a la semana, eliminándose la dependencia del horario de atención de la administración pública hacia la ciudadanía, permitiendo la interacción entre autoridades, ciudadanos, empresas y otras autoridades [2].
La implementación de dispositivos de identificación electrónica hace posible la eliminación de la tediosa práctica de llenar formularios en las instituciones, disminuyendo la asistencia personal de los ciudadanos

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 64-77 https://doi.org/10.33936/isrtic.v4i1.2348 | ISSN 2550-6730

a las oficinas públicas [30], permitiendo obtener la información del ciudadano desde un sistema central de información gubernamental posibilitando realizar trámites electrónicos a distancia eliminando considerablemente los incomodos desplazamientos y las largas colas de espera, reduciendo así la pérdida de tiempo en que los ciudadanos se ven afectados [11].

Gobierno electrónico y la sociedad [7][31] coinciden en la necesidad de las instituciones gubernamentales en actualizar sus servicios en línea para que puedan adaptarse a la tecnología del DNIe, se debe implementar proyectos que acerquen la administración pública a la sociedad y permitan a sus ciudadanos disminuir los trámites burocráticos de acreditación de identidad para el acceso a los servicios electrónicos, de esta forma el proceso de renovación del documento de identificación obligará por si solo a que la población tenga mayor acceso al dispositivo.

El gobierno electrónico es por lo tanto el proceso de aplicación de las Tecnologías de la Información y Comunicaciones para facilitar los procedimientos administrativos, según lo indica [30]. Lo destacable del DNIe de acuerdo a lo descrito por [7] son las implicaciones sociales que genera y las facilidades a los ciudadanos para el acceso a servicios electrónicos a través de la incorporación de una identidad digital, concepto que surge por la disponibilidad y adopción de las tecnologías de Internet las cuales allanaron el camino hacia los métodos actuales de transacciones en línea [32].

De la misma forma [2] aseveran que el gobierno electrónico permite la interacción entre autoridades, ciudadanos, empresas y otras autoridades, en la misma línea [28] exponen que la protección de datos y la prevención del fraude en línea son aspectos de gran importancia en ambientes de eGovernment.

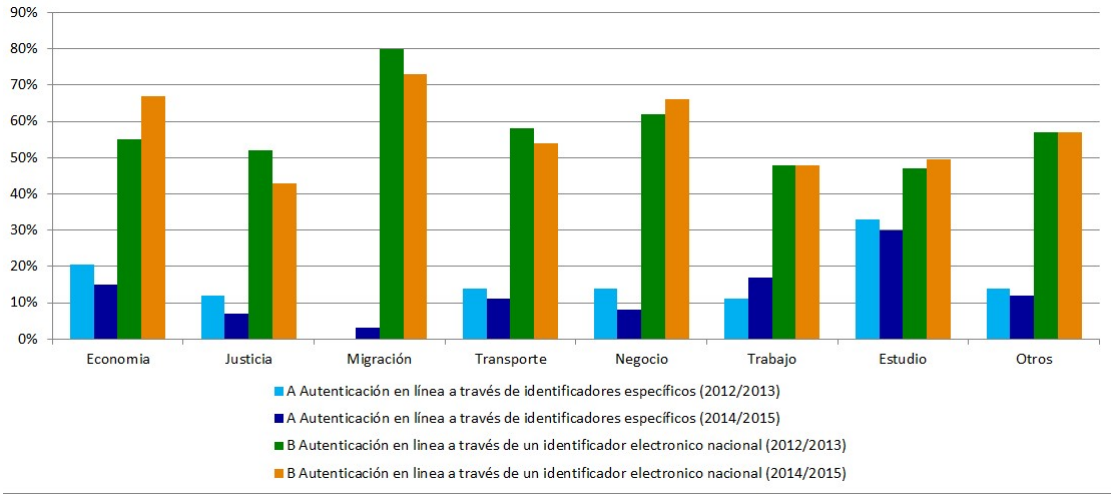

Figura 3: Uso de mecanismos de autenticación en 7 eventos de la vida (2012/2013 vs 2014/2015, EU28+, %)

Fuente: Adaptado de European Commission (2016)

En 2016 la European [33] estableció la necesidad de aumentar de manera más acelerada los servicios online en las administraciones públicas para satisfacer las expectativas de los ciudadanos y de las empresas, su informe proporciona información sobre el uso de medios de autenticación online. Se visualiza el aumento del uso del Identificador electrónico nacional para la autenticación de usuarios en siete eventos de la vida diaria de las personas en un periodo de análisis entre los años 2012 y 2015. En la figura 3 se detallan los resultados obtenidos.

Mientras que para el año 2018 la misma entidad confirmó que hubo un incremento del 34 % en la implementación de identificaciones electrónicas en los sitios web gubernamentales evaluados, de los cuales en el 18 % de estos se logró acceder a otro servicio sin necesidad de autenticarse nuevamente.

Países con dispositivos de identificación electrónica

Austria y Estonia son dos países referentes de Europa en términos de disponibilidad de gobierno electrónico, [30] indican que la mayor parte de los servicios de gobierno electrónico en Austria son accesibles a través de la web, mientras que Estonia lidera a nivel mundial la innovación de administración pública con una plataforma de voto electrónico online y una plan de residencia electrónica que incluye una tarjeta de identificación con chip, un lector de tarjetas y un generador de códigos con los cuales los residentes electrónicos pueden firmar documentos, identificarse y realizar trámites como por ejemplo la apertura de empresas en el país o el pago de impuestos sin necesidad de residir físicamente en el mismo [34].
Entre algunos ejemplos de implementaciones de soluciones de identidad electrónicas en Europa tenemos países como los referidos por [18] quien identificó a Finlandia como el primer país en emitir tarjetas electrónicas de identidad a sus ciudadanos en el año 1999 con el nombre de FinEID card, de la misma forma lo hizo Italia en el año 2001 implementando la CIE (Cartà d' Identita Elettronica), mientras que Bélgica empezó el plan piloto para emitir su EIC (Electronische Identiteitskaart) en el año 2003 según lo indicado por [35]. Australia también posee un documento de identidad similar denominado national document verification service (DVS) implementado a partir del año 2007 [36]
En Sudamérica Argentina es uno de los países que se encuentra migrando sus políticas de gobierno electrónico, un ejemplo de ello es que a partir del 1 de abril de 2017 el DNI digital será el único documento válido para autenticación en dicho país, teniendo un claro ejemplo de la transformación de la administración pública hacia la e-administración (Registro Nacional de las personas, 2017)
Es necesario señalar que el Ecuador se encuentra en un proceso de transformación de la administración pública hacia el gobierno electrónico, así lo demuestra la publicación de la [37] en donde se incluye al país en la segunda mejor categoría a nivel mundial con un alto nivel de participación electrónica sobre los servicios prestados por el gobierno coincidiendo con [38] quienes incluyen a Ecuador dentro de los países que están en proceso de transición hacia un nuevo sistema de identificación de próxima generación.
El Plan de Gobierno Electrónico en Ecuador de la Secretaria Nacional de la Administración Pública (2016) se incluye la organización del uso de certificados electrónicos y el desarrollo de la firma electrónica, existiendo tres instituciones vigentes calificadas para brindar servicios de certificación mediante infraestructura de clave pública como son el Banco Central del Ecuador, el Consejo de la Judicatura y la empresa privada Security Data. Cabe indicar que la empresa ANF Autoridad de Certificación Ecuador se encuentra en estado de liquidación [39]. En la figura 4 se muestra la estructura actual de la una de las entidades de certificación en Ecuador, el Consejo de la Judicatura:

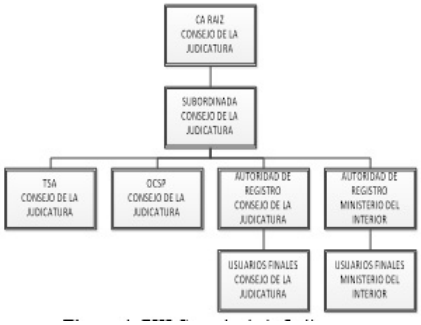

Figura 4: PKI Consejo de la Judicatura
Fuente: Adaptado de ARCOTEL (2016); Consejo de la Judicatura (2016)

Debilidades y amenazas del DNIe La conectividad de dispositivos móviles con el DNIe mediante tecnología NFC genera nuevos escenarios de amenazas, que no necesariamente dependen de la tecnología implementada en la tarjeta criptográfica, [40]confirmó la posibilidad de realizarse ataques de denegación de servicios a las infraestructuras PKI, por otra parte [41][42] propusieron una segunda forma de ataque mediante la instalación de aplicaciones ocultas en los dispositivos móviles (keylogger) la cual podría retransmitir información desde el dispositivo móvil de la víctima hacia otro destino (relay attack).

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 64-77 https://doi.org/10.33936/isrtic.v4i1.2348 | ISSN 2550-6730

[40] atribuía al factor humano como la mayor amenaza probable en un esquema de identificación electrónica, este error puede producirse al momento de enrolar el dispositivo por primera vez o al instante de tomar los datos biométricos para su registro en el chip.
Sin embargo, de acuerdo a las nuevas tendencias actuales en materia de investigación de criptoanálisis se confirma que la seguridad teórica implementada en las tarjetas criptográficas como el DNIe no garantiza su seguridad práctica debido a factores que no suelen ser tomados en cuenta al momento de diseñar el protocolo criptográfico esto a pesar de que según lo afirmado por [43] durante los últimos años se viene incrementando el uso de dispositivos electrónicos con características criptográficas para diversos fines (identificación personal, tarjetas de pago, etc.).
A los tipos de ataques cuyo objetivo es obtener información explotando las debilidades de los protocolos criptográficos de las tarjetas inteligentes se los denomina ataques de canal lateral (side cannel attacks) o por inducción de fallos (fault attacks), ejemplo de ello se tiene el conjunto de herramientas de software para ataques de canal lateral contra dispositivos criptográficos, en especial tarjetas inteligentes propuesto por [43].
De forma contraria, ante las eventuales debilidades presentadas en los sistemas criptográficos mediante la implementación de ataques de canal lateral, existen contramedidas que pueden ser aplicadas en diferentes niveles de abstracción de acuerdo a lo descrito por [44][45]

En el nivel físico: escudos, fuentes de alimentación desmontables para mejorar la resistencia de un dispositivo contra ataques físicos.
En el nivel tecnológico: CMOS alternativas para disminuir la dependencia de datos de consumo de energía.

En el nivel algorítmico: funciones de random, encriptación de buses, ocultación (utilizando retardos aleatorios, enmascaramiento de operaciones sensibles.

Para todos los niveles anteriores se puede incluso añadir ruido en amplitud como una solución genérica para disminuir la cantidad de información perdida por medio de canales laterales. De la misma forma existen las contramedidas en el nivel de protocolo, por ejemplo basadas en actualizaciones claves.

3. Conclusiones, Limitaciones y Trabajos Futuros

El dispositivo de identificación electrónica es un mecanismo de autenticación seguro considerado como un segundo factor de autenticación (algo que se sabe más algo que se tiene) el cual debe estar respaldado por una infraestructura de clave pública robusta para su correcta implementación. El dispositivo analizado es ideal para su aplicación en actividades electrónicas y comerciales en línea sin que existan restricciones de horarios, facilitando la prestación de servicios a los ciudadanos en ambientes de gobierno electrónico y generando confianza en las personas al saber que se posee una herramienta con la cual se evita el fraude y falsificación de identidades especialmente en Internet.
Ecuador posee una infraestructura de clave pública diversa, con instituciones gubernamentales y privadas que ofrecen servicios en el país, las cuales podrían aportar en conjunto en el proceso de la emisión de un nuevo documento de identificación electrónico acorde a las tendencias y estándares aplicados en otros países como el caso de la listas de servicios de confianza o Trusted Service List (TLS) en Europa.
Garantizar la accesibilidad a la información en un entorno de gobierno electrónico es un reto debido a la integración con tecnologías complejas como las tarjetas inteligentes, aun así, se avizora una importante implementación de dispositivos de identificación electrónica en áreas aún no tan difundidas como salud, justicia y voto electrónico, para lo cual es necesario que las instituciones públicas y privadas actualicen sus plataformas de servicios transaccionales online y de esta manera estar preparados ante una nueva herramienta de identificación nacional lo cual se traducirá en confianza por parte de los ciudadanos hacia

sus proveedores de servicios, el dispositivo permitirá entablar relaciones comerciales de gran nivel con cualquier parte del mundo teniendo los ciudadanos la seguridad que su identidad estará resguardada por una infraestructura robusta que deberá fortalecerse ante eventuales intentos de ataques electrónicos tan habituales hoy en día.

No se evidencia información oficial sobre la estructura interna de la actual cédula de identidad de Ecuador aunque en estudios referidos se establece que la misma incorpora características de almacenamiento de firma en fichas electrónicas, siendo ésta junto con el corto período de tiempo utilizado para la publicación las limitantes encontradas al momento de realizar una comparación cuantitativa con dispositivos de identificación electrónica implementados en otros países, por lo cual, para futuras investigaciones se propone realizar un análisis de laboratorio del documento de identificación vigente en Ecuador para definir la estructura del chip interno y las características que incorpora, adicional se recomienda realizar un estudio de las plataformas web en los distintos sectores de la administración pública para obtener un esquema actual de la gestión de gobierno electrónico con miras a su futura utilización.

Si bien es cierto, los sistemas criptográficos utilizados en la actualidad en los dispositivos de identificación electrónica como el caso del DNIe implementan tamaños grandes de claves que conllevan mucho esfuerzo invertido (tiempo y dinero) para poder descifrarlas y con los cuales se puede estar seguro por un buen tiempo, no es menos cierto que los actuales avances tecnológicos en materia de investigación de ataques de canales laterales se encuentra en aumento, por lo que habrá que estar atentos al constante avance tecnológico para establecer contramedidas en el momento en que se detecten debilidades y vulnerabilidades en los sistemas de cifrado actuales.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 64-77 https://doi.org/10.33936/isrtic.v4i1.2348 | ISSN 2550-6730

Referencias

[1] A. Corletti. "Seguridad en Redes". En: (2016).

[2] Flavio Corradini, Eleonora Paganelli y Alberto Polzonetti. "The e-Government digital credentials". En: *International Journal of Electronic Governance* 1.1 (2007), págs. 17-37.

[3] V. Gayoso Martínez, L. Hernández Encinas y A. Martín Muñoz. "La tarjeta de identidad española como método de autenticación en redes sociales". En: *VII Congreso Iberoamericano de Seguridad Informática*. 2013, págs. 32-44.

[4] Kaspersky. *Kaspersky registra 45 ataques por segundo en América Latina.* 2019. URL: `https://latam.kaspersky.com/blog/kaspersky-registra-45-ataques-por-segundo-en-america-latina/15274/`.

[5] Luis Gerardo Gabaldón y Wílmer Pereira. "Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico". En: *Sociologias* 20 (2008), págs. 164-190.

[6] Amos Fiat y Adi Shamir. "How to prove yourself: Practical solutions to identification and signature problems". En: *Conference on the theory and application of cryptographic techniques*. Springer, 1986, págs. 186-194.

[7] Javier Crespo Sánchez y col. "Hacia una nueva identificación electrónica del ciudadano: el DNI-e". En: (2006).

[8] Jordi Forne. "Criptografia y seguridad en comunicaciones". En: *Novática: Revista de la Asociación de Técnicos de Informática* 116 (1995), pág. 20.

[9] Simson Garfinkel, Gene Spafford y Mario Camou Riverol. *Seguridad y Comercio en el Web*. McGraw-Hill, 1999.

[10] Tomàs Baiget. "DNI electrónico (DNIe)". En: *Anuario ThinkEPI* 1 (2007), págs. 203-204.

[11] E. Directivos. "Características y funciones del DNI electrónico." En: (2008). URL: `http://search.ebscohost.com/login.aspx?direct=trueydb=fuayAN=40074735ylang=esysite=ehost-live`.

[12] Javier Espinosa-Garcia, L. Hernández Encinas y A. Queiruga Dios. "The new Spanish electronic identity card: DNI-e". En: *Conference on Cryptology and Digital Content Security*. 2007.

[13] R. Sarwat. "DNI-e Tecnología y Usos". En: *Móstoles, Madrid*. 64 (2010).

[14] Kevin Curran, Amanda Millar y Conor Mc Garvey. "Near Field Communication." En: *International Journal of Electrical & Computer Engineering (2088-8708)* 2.3 (2012).

[15] Jose Maria León-Coca y col. "Authentication systems using ID Cards over NFC links: the Spanish experience using DNIe". En: *Procedia Computer Science* 21 (2013), págs. 91-98.

[16] V. Gayoso Martínez y col. "A comparative study of three Spanish eGoverment smart cards". En: *Logic Journal of the IGPL* 25.1 (2017), págs. 42-53.

[17] Whitfield Diffie y Martin Hellman. "New directions in cryptography". En: *IEEE transactions on Information Theory* 22.6 (1976), págs. 644-654.

[18] Niklas Auerbach. "Anonymous digital identity in e-government". PhD Thesis. University of Zurich, 2004.

[19] Rolando Chaparro, Pablo Greenwood y Benjamín Barán. *Alternativa de Infraestructura de Clave Pública Basada en el uso de DNSSEC*. 2008.

[20] C. Adams. "Trusted Third Party. In H. C. A. van Tilborg y S. Jajodia (Eds.)" En: *Encyclopedia of Cryptography y Security* (), págs. 1335-1335.

[21] Marc Girault y Self-Certified Public Keys. "Advances in Cryptology-EUROCRYPT'91". En: *LNCS* 547 (1991), págs. 490-497.

[22] Gladys Stella Rodríguez. "La certificación electrónica venezolana: Desde una perspectiva reflexiva". En: *Revista de Derecho* 17.17 (2011).

[23] Emilia P. Belleboni y Justo Carracedo Gallardo. "Uso del DNIe para reforzar el anonimato en el voto telemático mediante tarjetas inteligentes". En: ().

[24] Rubén González Crespo y col. "Design of an Open Platform for Collective Voting through EDNI on the Internet". En: *E-Procurement Management for Successful Electronic Government Systems*. IGI Global, 2012, págs. 1-13.

[25] J. A. Gutierrez-de-Mesa y col. "The Cost of Development of a New System to Control Drivers using GPS location and Identification through the electronic ID card". En: (2009).

[26] Igor Ruiz-Agundez y Pablo G. Bringas. "Service authentication via electronic identification cards: voip service authentication through the DNIe". En: *2012 Annual SRII Global Conference*. IEEE, 2012, págs. 602-607.

[27] Luis Enrique Sanchez y col. "LOPD Compliance and ISO 27001 legal requirements in the Health Sector". En: *IEEE Latin America Transactions* 10.3 (2012), págs. 1824-1837.

[28] David Arroyo y col. "Using smart cards for authenticating in public services: A comparative study". En: *Advances in Intelligent Systems and Computing* (2015).

[29] Ana Nieto, Rodrigo Roman y Javier Lopez. "Testigo digital: delegación vinculante de evidencias electrónicas para escenarios iot". En: *II Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2016)* 6 (2016), pág. 2016.

[30] Clemens Orthacker y Thomas Zefferer. "Accessibility challenges in e-Government: an Austrian experience". En: *Proceedings of the Forth International Conference on Internet Technologies and Applications (ITA 2011)*. 2011, págs. 221-228.

[31] Pablo R. Prieto. "El DNI electrónico: ecosistema y uso en la e-administración local". En: *El profesional de la información* 20.3 (2011), pág. 277.

[32] J. L. Camp. "Digital identity". En: *IEEE Technology and society Magazine* 23.3 (2004), págs. 34-41.

[33] E. Commission. "eGovernment Benchmark 2016". En: 80 (2016). URL: `https://www.capgemini.com/resources/egovernment-benchmark-2016`.

[34] G. Estonia. "The digital society." En: (2016). URL: `https://e-estonia.com/e-residents/about/`.

[35] Alea Fairchild. "The Evolution of the e-ID card in Belgium: data privacy and multi-application usage". En: *Sixth International Conference on Digital Society*. 2012.

[36] Organisation for Economic Co-operation y Development. *National strategies and policies for digital identity management in OECD countries*. OECD Publishing, 2011.

[37] ONU. "United Nations e-goverment survey 2016." En: *New York: Department of Economic and Social Affairs* (2016). URL: `http://workspace.unpan.org/sites/Internet/Documents/UNPAN96407.pdf`.

[38] ITU. *Review of National Identity Programs*. 2016. URL: `https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/09_2016/Review%20of%20National%20Identity%20Programs.pdf`.

[39] Arcotel. "Registro Publico de Entidades de Certificacion y Terceros Vinculados." En: (2016). URL: `http://www.arcotel.gob.ec/entidades-de-certificacion-firma-electronica/`.

[40] Siddhartha Arora. "National e-ID card schemes: A European overview". En: *Information Security Technical Report* 13.2 (2008), págs. 46-53.

[41] Julio José Píñar Figueroa y José Camacho Páez. "Pago móvil mediante NFC: Estudio y modelo de vulnerabilidad". En: (2016).

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 64-77 https://doi.org/10.33936/isrtic.v4i1.2348 | ISSN 2550-6730

[42] Michael Roland, Josef Langer y Josef Scharinger. "Practical attack scenarios on secure element-enabled mobile devices". En: *2012 4th International Workshop on Near Field Communication*. IEEE, 2012, págs. 19-24.

[43] Alberto Fuentes y col. "Design of a Set of Software Tools for Side-Channel Attacks". En: *IEEE Latin America Transactions* 13.6 (2015), págs. 1966-1978.

[44] Stefan Mangard, Elisabeth Oswald y Thomas Popp. *Power analysis attacks: Revealing the secrets of smart cards*. Vol. 31. Springer Science & Business Media, 2007.

[45] François-Xavier Standaert. "Introduction to side-channel attacks". En: *Secure Integrated Circuits and Systems*. Springer, 2010, págs. 27-42.