InterSedes, *Revista electrónica de las sedes regionales de la Universidad de Costa Rica*,
ISSN 2215-2458, Volumen XXIV, Número 50, Julio-Diciembre, 2023.
10.15517/isucr.v24i50.50329 | intersedes.ucr.ac.cr | intersedes@ucr.ac.cr

InterSedes

ESP Editorial Sede del Pacífico

Implementación de un sistema de cédula electrónica en Colombia

Implementation of an electronic card system in Colombia

Fredy Yesid Ávila Niño
Escuela de Policía Rafael Reyes
Boyacá, Colombia
segundo.avila@correo.policia.gov.co

Resumen: En el artículo se describen diferentes casos en los cuales se ha llevado a cabo una implementación exitosa de un sistema de identificación digital, en donde se realizó un análisis de los elementos que la componen y se propone un esquema para la implementación de un sistema de cédula electrónica en Colombia. Del mismo modo se estudiaron las teorías y conceptos que se deben tener en cuenta para que dicha implementación pueda llevarse a cabo dentro de los estándares internacionales y que beneficie al estado y a la ciudadanía en general. Por lo tanto, es importante analizar este tipo de sistema de identificación en países donde su implementación ha sido exitosa y que para el estudio se utilizaron como referencia: España, Italia, Perú y Uruguay, de tal forma que ha sido posible identificar características y elementos de seguridad que se puedan incorporar al sistema de cédula electrónica en Colombia.
A través de una revisión documental y realizando la consulta en los portales oficiales de los gobiernos de diferentes países, así como de las entidades encargadas de identificar a los ciudadanos, se identificaron diferentes países en donde la transición de un sistema de identificación tradicional hacia un sistema de identificación digital generó un impacto positivo y se redujeron los problemas de seguridad que serán explicados más adelante.
El presente documento se obtiene de la investigación realizada en el desarrollo del trabajo de grado: "Implementación de un sistema de cédula electrónica en Colombia para identificación digital".

Palabras clave: cédula electrónica, certificado digital, firma electrónica, identificación digital, gobierno en línea.

Abstract: The article describes different cases in which a successful implementation of a digital identification system has been carried out, where an analysis of the elements that compose it was carried out and a scheme for the implementation of a card system is proposed. electronics in Colombia. In the same way, the theories and concepts that must be taken into account so that said implementation can be carried out within international standards and that benefit the state and citizens in general were studied.
Therefore, it is important to analyze this type of identification system in countries where its implementation has been successful and which were used as a reference for the study: Spain, Italy, Peru and Uruguay, in such a way that it has been possible to identify characteristics and elements. that can be incorporated into the electronic ID system in Colombia.
Through a documentary review and consulting the official portals of the governments of different countries, as well as the entities in charge of identifying citizens, different countries were identified where the transition from a traditional identification system to a of digital identification generated a positive impact and the security problems that will be explained later were reduced.
This document is obtained from the research carried out in the development of the degree work: "Implementation of an electronic ID system in Colombia for digital identification".

Keywords: electronic ID, digital certificate, electronic signature, digital identification, online government

Recibido: 4-03-22 | Aceptado: 31-08-22

Cómo citar (APA): Ávila Niño, F. (2023). Implementación de un sistema de cédula electrónica en Colombia. InterSedes, 24(50), 190-224. DOI 10.15517/isucr.v24i50.50329

Publicado por la Editorial Sede del Pacífico, Universidad de Costa Rica

1. Introducción

Es importante mencionar que cualquier ciudadano nacido en Colombia, por derecho propio adquiere los derechos y obligaciones del país, y uno de esos derechos que el estado colombiano otorga es la de identificarlo legalmente, inicialmente se realiza dicha identificación a través de un registro civil de nacimiento, el cual es expedido por la Registraduría Nacional del Estado Civil, cuyo Número Único de Identificación Personal (*NUIP*), será el mismo número que lo identificará en la tarjeta de identidad (documento para menores de edad), cédula de ciudadanía, pasaporte y en el caso de los hombres en la libreta militar. Registraduría Nacional del estado Civil (2012).

En Colombia, la cédula de ciudadanía nace a partir de la necesidad de identificar a las personas al momento de votar, posteriormente como documento de identificación. Debido a su importancia dentro del sistema electoral, el proceso de cedulación se designa a una entidad autónoma, la Registraduría Nacional del Estado Civil (*RNEC*). A través del decreto 1010 del 2000, se establece su organización y las funciones, dentro de las cuales se tiene: "Expedir y elaborar las cédulas de ciudadanía de los colombianos, en óptimas condiciones de seguridad, presentación y calidad y adoptar un sistema único de identificación a las solicitudes de primera vez, duplicados y rectificaciones." Decreto 1010 (2000).

La evolución de este documento se caracteriza por la implementación de medidas de seguridad; es decir, la cédula ha incorporado en el documento físico diferentes medidas para evitar su falsificación y garantizar la plena identificación del ciudadano. Desde el año 2000 se expide lo que la Registraduría ha denominado Cédula de Ciudadanía de tercera y última generación, la cual se ha basado en el sistema de identificación mediante la tecnología AFIS (*Automated Fingerprint Identification System*).

No obstante, este documento actualmente no logra garantizar la plena identidad de los ciudadanos, ya que cada vez es más frecuente tener casos de suplantación de identidad con documentos falsificados, lo cual es una situación que representa un alto riesgo para las personas. Por otra parte, los avances en cuanto a

tecnología han permitido que en diferentes países como: España, Alemania, Italia, Bélgica, Israel, Uruguay, Perú y Chile, ya cuentan con cédula digital.

En este aspecto el estado colombiano debe iniciar la transición hacia un sistema de identificación electrónica que le permita complementar los lineamientos establecidos en los servicios ciudadanos digitales: "el cuál está compuesto de los servicios de autenticación digital que incluye la autenticación digital con cédula digital y el servicio de validación de identidad biométrica ante Registraduría, la carpeta ciudadana y la interoperabilidad." Decreto 1413 (2017).

A partir de lo anteriormente expuesto, se propone un modelo que pueda servir como punto de referencia para implementar en Colombia la cédula electrónica, esto a partir del estudio e identificación en casos exitosos de otros países de los factores fundamentales a tener en cuenta en este proceso.

El presente artículo está enfocado en realizar un análisis de los casos en donde se ha implementado de manera exitosa la cédula electrónica, particularmente en España, Perú, Chile y Uruguay, de tal forma que sea posible generar una guía que permita establecer el procedimiento para que el estado colombiano modernice el sistema de identificación. Con esto el país tendrá la capacidad de:

- Mejorar y fortalecer la estrategia de gobierno en línea. Es importante para el estado impulsar la estrategia gobierno en línea y obtener el máximo provecho de los cuatro componentes que la componen: TIC para servicios, TIC para Gobierno Abierto, TIC para la Gestión y Seguridad y Privacidad de la Información. Ministerio de las Tecnologías de la información y las Comunicaciones (2018).

- Avanzar en cuestiones de transformación digital. Proporcionar un mecanismo que permita la plena identificación de los ciudadanos, con mecanismos de seguridad y eliminar el riesgo de suplantación de identidad y falsificación de documentos.

InterSedes, ISSN 2215-2458, Volumen 24, Número 50-
Julio-Diciembre, 2023, pp. 190-224 (Artículo).

- Proporcionar comodidad al ciudadano. La identidad digital le permite al ciudadano eliminar barreras que con frecuencia hacen que los servicios proporcionados por el gobierno sean complicados o de difícil acceso. Debido a la capacidad que ofrece la identificación digital, los ciudadanos pueden acceder a muchos de estos servicios sin tener que estar físicamente presentes en la mayoría de los casos. Por otra parte, adoptando los enfoques de prestación de servicios en línea, los ciudadanos se benefician de la disponibilidad de servicios 24 horas al día, 7 días a la semana.

- Reducir costos de acceso a los servicios. Los ciudadanos al no tener que realizar el desplazamiento físico hasta la sede de la entidad de gobierno en la que va a realizar determinado tramite, reduce los costos indirectos que se generan al acceder a los servicios. Otro aspecto es la eliminación de solicitud de copias del documento físico para soportar la realización del trámite, en Colombia es muy frecuente que se solicite fotocopia del documento de identidad para diferentes tramites (bancarios, entidades prestadoras de salud, entidades de estado, etc.) con el documento de identificación digital este costo se evita y también el riesgo que se genera al generar fotocopias del documento que ser utilizadas para otros fines.

- Mejorar la prestación de servicios. El propósito de implementar un sistema de identificación electrónico es mejorar las condiciones de la sociedad en general y de los ciudadanos. Esto a través de la prestación de un mejor y más efectivo servicio, en Colombia se ha establecido una estrategia definida por el Gobierno Nacional mediante el Decreto 1151 (2008), que pretende lograr un salto en la inclusión social y en la competitividad del país a través de la apropiación y el uso adecuado de las Tecnologías de la Información y las Comunicaciones. Por lo tanto, un sistema de identificación moderno y acorde a la estrategia es requerido para aprovechar de mejor manera las herramientas con las que el Estado.

- Optimización de recursos. El nuevo sistema de identificación ayudará a las instituciones o entidades del estado a optimizar y utilizar de manera eficiente los recursos destinados a programas sociales y de bienestar. Esto debido a que el gobierno y la administración pública evitan que se asignen recursos a personas que no pueden ser beneficiadas, puesto que pueden existir suplantaciones o registros erróneos en las bases de datos de los beneficiarios.

- Mejorar la seguridad. La identidad digital contribuye en gran medida a incrementar el nivel de seguridad del Estado, ya que se constituye en una herramienta eficaz para la policía y el enjuiciamiento de delitos, y puede lograr que se aumente la eficacia de la lucha contra delitos específicos como fraudes de identidad, fraudes fiscales, entre otros.

La actual cédula de ciudadanía en Colombia es el documento con el que los ciudadanos colombianos se identifican, este año cumplirá 22 años puesto que se ha expedido desde mayo del año 2000, por lo tanto, las necesidades han cambiado y la tecnología ha avanzado hasta permitir un nuevo sistema de identificación electrónica, la cual entre otras cuestiones permite:

- Almacenamiento de información: Mediante un chip integrado en el documento físico es posible almacenar los datos del ciudadano.

- Firma electrónica: Incorpora un certificado electrónico valido.

- Identificación en sedes electrónicas: El estado colombiano cuenta con una estrategia de gobierno en línea, mediante la cual se establecen algunas sedes electrónicas y tramites que se pueden realizar por internet.

- Sello electrónico: Este sello también está basado en el certificado electrónico.

InterSedes, ISSN 2215-2458, Volumen 24, Número 50-
Julio-Diciembre, 2023, pp. 190-224 (Artículo).

- Código seguro de verificación (CSV): Es un código estampado en el documento físico que permite la verificación de la autenticidad e integridad de este.

- Evita la suplantación: El certificado digital generado para cada ciudadano es único, lo que permite garantizar la no suplantación.

- Portabilidad: El ciudadano puede habilitar en el móvil la cedula electrónica y esta tiene la misma validez que el documento físico.

2. Referente teórico

En este apartado se presentarán los fundamentos teóricos y conceptuales sobre los cuales se sustentará esta investigación, Inicialmente se realizará una reseña de la cédula de ciudadanía en Colombia, sus inicios y evolución, esto con el fin de conocer el proceso que se ha llevado a cabo en cuanto a identificación y las mejoras que se han implementado en las diferentes versiones del documento de identidad, posteriormente se mencionaran aspectos relevantes del programa de modernización tecnológica de la Registraduría Nacional del estado Civil. Un aspecto fundamental del desarrollo de la investigación es identificar los problemas de seguridad que se encuentran en el actual sistema de identificación. En la siguiente fase de la construcción del estado del arte se mencionarán los elementos que hacen parte del sistema electoral, así como los componentes del documento electrónico, posteriormente es importante establecer el marco normativo que existe en el país en cuanto a la identificación digital, también se deben tener en cuenta los estándares internacionales que aplican para el caso de estudio.

2.1 Cédula de ciudadanía en Colombia

En Colombia, la cédula de ciudadanía es el documento mediante

el cual se identifican los ciudadanos colombianos mayores de 18 años. Esto aplica para los colombianos por nacimiento o adopción; es decir, por adopción es el tipo de nacionalidad que se otorga, por parte del Gobierno colombiano a extranjeros a través de la Carta de Naturaleza o de una Resolución de Inscripción.

La Ley 39 de 1961, por la cual se dictan normas para la cedulación, y otras de carácter electoral, dispuso en su artículo primero que: "a partir del primero de enero de mil novecientos sesenta y dos (1962), los ciudadanos colombianos que hayan cumplido veintiún años solo podrán identificarse con la cedula de ciudadanía laminada, en todos los actos civiles, políticos, administrativos y judiciales" Ley 39 (1961).

2.1.1 Antecedentes históricos

En Colombia en sus inicios a la cédula de ciudadanía era conocida como *título del elector*, este documento de identificación surgió como el elemento necesario y fundamental para poder ejercer el derecho al voto y con el paso del tiempo como instrumento para validar la identidad. Esta situación conllevo a que, en los diferentes códigos electorales, el proceso de cedulación se incluyera como un elemento estructural o columna vertebral del sistema electoral del estado colombiano. Al constituirse como instrumento fundamental del proceso electoral, el proceso de cedulación se designa constitucionalmente a una entidad que opere de manera independiente de las ramas del poder público, a la Registraduría Nacional del Estado Civil.

2.1.2 Problemas de seguridad en el actual sistema de identificación

Los documentos de identidad tal y como se conocen hoy en día en Colombia, han sido diseñados e implementados en una época diferente, puesto que hace 22 años los mecanismos de seguridad que se han incorporado en el documento físico, puede que ya no resulten tan seguros, toda vez que con los avances tecnológicos los delincuentes han conseguido falsificar cédulas.

InterSedes, ISSN 2215-2458, Volumen 24, Número 50-
Julio-Diciembre, 2023, pp. 190-224 (Artículo).

Actualmente el sistema de identificación en Colombia presenta algunas falencias que son:

Suplantación de persona / de identidad: Esta situación se produce cuando un ciudadano intenta conseguir una cédula de ciudadanía a nombre de otra persona. Esto es mejor conocido como *robo de identidad*, lo cual consiste en que cierta persona logra obtener otros documentos como el pasaporte hasta tramitar créditos bancarios a nombre de otro ciudadano colombiano, incluso se han conocido múltiples casos de venta de bienes inmuebles propiedad de terceros. Para analizar casos de este tipo, la Registraduría Nacional del Estado Civil cuenta con el apoyo y asesoría de dactiloscopistas especializados, que emiten un concepto técnico y a partir de esto el caso es trasladado a los lugares donde se preparan las cédulas, con el fin de que se adelanten las acciones pertinentes ante la Fiscalía General de la Nación. En el apartado de falsificación de documentos se detalla la manera en la que los delincuentes realizan esta suplantación.

Doble cedulación: Cuando algún ciudadano intenta conseguir dos o más cédulas de ciudadanía a su nombre, pero con diferente cupo numérico. En este caso los documentos contienen las mismas huellas dactilares y hasta el mismo nombre o la misma fotografía, pero finalmente se trata de dos documentos completamente distintos. Para que no existan casos de doble cedulación se debe expedir una resolución de cancelación de uno de los dos documentos vigentes.

Información defectuosa causada por inconsistencias o fallas en la calidad: Este tipo de cédulas no es posible expedirlas debido a que la información proporcionada por el ciudadano no coincide o presenta inconsistencias con respecto a la que reposa en las bases de datos de la Registraduría Nacional del Estado Civil. Cuando se producen este tipo de casos el ciudadano interesado debe acudir a la Registraduría para repetir el trámite de solicitud de este documento. Las inconsistencias que se presentan con mayor frecuencia son:

- El ciudadano modificó su sexo, situación que no se tramita a través de obtener un duplicado de la cédula.

- El tipo de sangre o grupo sanguíneo informado por el ciudadano no coincide con el que se encuentra registrado en la base de datos.

- La impresión de las huellas dactilares es de baja calidad o son defectuosas, por dermatitis, uso frecuente de químicos, resequedad, etc.

- La fotografía es de baja calidad o presenta algún defecto.

- La firma está recortada o de baja calidad.

En estos casos el trámite del documento toma mucho más tiempo del que normalmente tarda, esto demanda realizar nuevamente todo el proceso y puede tomar hasta seis meses, incluso más tiempo. De tal modo que se ve afectado el ciudadano, puesto que no portará el documento de identificación legal y para muchos procesos es requerido contar con la cédula.

Falsificación de documentos: El documento más falsificado en Colombia es la cédula de ciudadanía, esto debido a que genera algún tipo de ganancia o beneficio inmediato, por ejemplo, tramite de préstamos o acceso a planes de telefonía celular u otros servicios que le generen interés a los falsificadores.

Tipos de suplantación y falsedad en cédulas, de acuerdo con Lozada (2020) de Infolaft, en Colombia existen tres tipos de suplantación en lo que se refiere a las cédulas de ciudadanía:

- **Integral**: En este tipo de suplantación, clonan los datos reales de la persona y los consignan en un documento falso, adicionalmente insertan la foto y huella del suplantador. Esta modalidad es muy utilizada ya que las bases de datos no detectan esta suplantación porque los datos son reales.

InterSedes, ISSN 2215-2458, Volumen 24, Número 50-
Julio-Diciembre, 2023, pp. 190-224 (Artículo).

- **Parcial**: Retiran la lámina protectora del documento original, posterior a eso le cambian la fotografía y la huella mediante un moderno sistema de escáner e impresión. No se altera ningún otro aspecto de la cédula de ciudadanía, teniendo como resultado un documento que difícilmente pueda ser detectado por las entidades, incluso por la autoridad, ya que al verificar el documento a través del código de barras bidimensional (ubicado en la parte posterior de la cédula) aparecen los datos de la persona suplantada.

- **Inocua**: Es cuando se elabora el documento en una imprenta ilegal, pero en este caso se entrega al titular de los datos. No se constituye una suplantación, pero si se porta un documento falsificado, porque el ciudadano paga a un tramitador para que le expida el documento con sus datos reales, pero la cédula es falsa porque no fue elaborada por la Registraduría.

2.1.3 Elementos que hacen parte de un sistema de identificación electrónica.

La identificación electrónica debe tener en cuenta el concepto de identidad conceptualizada desde el punto de vista del uso de la tecnología, mediante elementos encargados de garantizar la unicidad de una persona física y por elementos que son la expresión de la identidad humana en todos sus posibles aspectos, teniendo en cuenta aspectos legales, se establece: "que la identidad personal está formada, tradicionalmente, por el conjunto de datos resultantes de la unión de la información relativa a una persona presente en los registros públicos que va a permitir identificarla de forma unívoca" (Sánchez, 2016).

La Unión Europea se ha pronunciado frente a la protección de datos, y ha desarrollado con el propósito de otorgar a la persona un mayor control sobre su identidad y sus datos personales; se plantean un conjunto de requisitos que se deben cumplir por: receptores, controladores, procesadores y terceras partes al momento de manejar dichos datos. El artículo 2, letra a) define datos personales de la siguiente manera:

> Datos personales: toda información sobre una persona física identificada o identificable (el interesado); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social. Directiva Europea 95/46/CE (1995, p. 34).

Identidad Digital

La Unión Internacional de Telecomunicaciones define el concepto de identidad como una representación de una entidad en forma de uno o más atributos que permiten que la entidad o entidades se distingan suficientemente dentro del contexto. Partiendo de esta definición, es posible afirmar que una identidad digital es la representación digital de una entidad, lo suficientemente detallada para que el individuo se distinga dentro el contexto digital.

La identidad es un elemento crucial para cada individuo, ya que define e identifica los rasgos principales de cada uno y cada persona. Obviamente, la identidad digital es igualmente importante. Conserva las características intrínsecas que hacen de la identidad un factor tan determinante y, al mismo tiempo, puede verse como una herramienta que Los estados y gobiernos pueden aprovechar para satisfacer las demandas de sus ciudadanos o para mejorar su eficiencia global.

Dada la importancia primordial que la identidad digital puede tener en un contexto nacional, los líderes nacionales y los formuladores de políticas deberían considerar la implementación de un marco específico, a saber, un marco de identidad, que comprende todos los elementos necesarios para operar un Sistema de Identidad Digital y entregar su servicio a la población.

Elementos de la Identidad Digital

Como se indica en la definición anterior, una entidad se repre-

InterSedes, ISSN 2215-2458, Volumen 24, Número 50-
Julio-Diciembre, 2023, pp. 190-224 (Artículo).

senta a través de uno o más *atributos*. Estrictamente hablando, un atributo se puede definir como un *elemento de datos específico perteneciente a un individuo*. Los atributos pueden considerarse como los componentes básicos de una identidad digital. Se pueden dividir en diferentes categorías, como información relacionada con el nacimiento (nombre, lugar de nacimiento, fecha de nacimiento, etc.), información descriptiva (altura, peso, rasgos físicos, etc.), identificadores personales (por ejemplo, número de seguro social), datos biométricos (huella dactilar, ADN, iris, etc.), etc.

3. Metodología

A partir de una investigación detallada sobre la cédula electrónica y el sistema de identificación en Colombia, se busca proponer el procedimiento mediante el cual pueda establecerse una base que permita la implementación de la cédula electrónica en el país.

Inicialmente se realizó la definición del problema identificado y que fue objeto de estudio, posteriormente se establece del alcance del proyecto, es importante conocer el estado actual y la evolución del documento de identificación en Colombia, toda vez que es relevante identificar la manera en la cual se lleva a cabo el proceso de identificación de los ciudadanos en el país, con esto se logra comprender las necesidades por parte del estado en cuanto a la identificación de las personas.

Una buena práctica es referenciarse en países que ya han hecho la transición del documento de identidad convencional a uno electrónico, para identificar los elementos que se han incorporado en cada uno de ellos y analizar cuáles pueden ser incluidos en la propuesta a realizar. De acuerdo con la experiencia de los países que se toman como referencia es posible resaltar las fortalezas de cada caso y tomar lo mejor de cada uno de ellos para adaptarlos a las necesidades propias.

Finalmente se realiza un análisis que permita evaluar la viabilidad para el país en cuanto a la implementación de la cédula electrónica para la identificación, ya que el aporte del consiste en identificar los elementos a tener en cuenta al momento de definir

los componentes de este tipo de documentos y que del mismo modo logren suplir las necesidades del estado colombiano en cuanto a la identificación y a la articulación de los servicios del gobierno en línea, adicionalmente es posible identificar que otro tipo de servicios o tramites se llevarían de mejor manera si los ciudadanos de Colombia portaran un documento con estas características.

3.1 Enfoque

El enfoque de la investigación es cuantitativo, debido a que se realizó una valoración de los casos relevantes de implementación de sistemas de identificación digital. El alcance del estudio es descriptivo ya que identificó indicadores y características propias de cada caso que permitieron definir un conjunto de recomendaciones para que el sistema de identificación propuesto cuente con las características tecnológicas y de seguridad que le permitan cumplir con los estándares y normas vigentes.

3.2 Población de estudio

Se realizó un levantamiento de información sobre casos relevantes en cuanto a la implementación de sistemas de identificación digital a nivel mundial, en donde inicialmente se estudiaron los casos de: Afganistán, Alemania, Bélgica, Chile, España, Filipinas, Guatemala, Indonesia, Italia, Israel, Perú, Uruguay. Con la intención de delimitar el estudio y gracias al levantamiento de información realizado se toman en concreto y como referencia los sistemas de identificación de: España, Italia, Uruguay y Perú.

3.3 Técnicas de recolección

Se realizó una revisión documental sobre los sistemas de identificación digital con el propósito de conocer casos exitosos en los cuales se el País ha realizado la transición de una identificación tradicional a una digital, lo que permitió adquirir un mayor conocimiento del tema y estructurar una propuesta que contiene los elementos tecnológicos y de seguridad apropiados para una cédula

InterSedes, ISSN 2215-2458, Volumen 24, Número 50-
Julio-Diciembre, 2023, pp. 190-224 (Artículo).

electrónica. Por otra parte, se profundizo sobre casos puntuales como lo son: España, Italia, Uruguay y Perú.

DNI electrónico (DNIe) – España

El Documento Nacional de Identidad electrónico o DNIe, emitido en España desde marzo de 2006 por la Dirección General de la Policía. Su característica principal es la incorporación un chip con capacidad para almacenar la misma información impresa en la tarjeta de forma segura, imágenes digitalizadas de la fotografía, la firma manuscrita y las impresiones dactilares, adicionalmente los certificados digitales para la autenticación y firma electrónica. El DNIe no almacena ningún otro dato personal diferente a los que se encuentran impresos, como pueden ser los datos e información sanitaria, judicial, fiscal, policial, penal, etc.

Los ciudadanos españoles con el DNIe pueden realizar trámites en los organismos gubernamentales, efectuar transacciones de manera segura con entidades bancarias y participar en sesiones de videoconferencia a través de Internet con la convicción de la identidad de los interlocutores. Entre las ventajas del DNI electrónico se destacan las siguientes:

- Seguridad: Es mucho más seguro que el documento anterior, incorpora mayores medidas de seguridad, lo cual hace que sea casi imposible falsificarlo.

- Comodidad: Permite que los ciudadanos puedan realizar trámites a distancia y en cualquier momento (24 / 7).

- Ergonomía: Es mucho más robusto, está fabricado en policarbonato y se estima que el ciclo de vida útil es de unos diez años. Además, mantiene las dimensiones del DNI tradicional.

Características de la tarjeta electrónica

El DNI certifica de manera física y electrónica la identidad del

titular y los datos personales que se encuentran allí consignados. El objetivo de la parte electrónica del DNI es incorporar en el documento todas las capacidades criptográficas que son necesarias para que se permita acreditar la identidad electrónica asociada al titular del documento. Una vez se ha establecido esa identidad y es asociada a los elementos criptográficos del DNI es posible demostrar electrónicamente la identidad del ciudadano. La identidad electrónica avalará todas aquellas actuaciones y actividades que se puedan asociar a esta.

Características del Chip:

- Modelo: SLE78CLFX408AP de Infineon Technologies, Sistema operativo: DNIe v4.0 / Versión comercial DNI 3.0), 400KB memoria Flash (código + personalización), 8 KB memoria RAM, Interfaz Dual (con contacto / sin contacto), Criptolibrería RSA y CC EAL5+.
- Contenido: La información en el chip está distribuida en tres zonas con diferentes niveles y condiciones de acceso:
- Zona pública: Accesible en lectura sin restricciones, contenido: Certificado x509 de componente, Certificado CA intermedia emisora, Claves Diffie-Hellman.
- Zona privada: Accesible en lectura por el ciudadano, mediante la utilización de la Clave Personal de Acceso o PIN, conteniendo:
- Certificado de Autenticación (Digital Signature), Certificado de Firma (No Repudio).

El chip de la tarjeta almacena los siguientes certificados electrónicos:

- Certificado de Componente. Su propósito es la autenticación de la tarjeta del DNIe mediante el protocolo de autenticación mutua definido en CWA 14890. Permite el establecimiento de un canal cifrado y autenticado entre la tarjeta y los Drivers. Este certificado no estará accesible

InterSedes, ISSN 2215-2458, Volumen 24, Número 50-
Julio-Diciembre, 2023, pp. 190-224 (Artículo).

directamente por los interfaces estándar (PKCS#11 o CSP).

- Certificado de Autenticación. Este certificado es el que se utiliza para establecer el canal seguro con autenticación de Cliente/Servidor. Es un certificado X509v3 estándar, que tiene activo en el Key Usage el bit de Firma Digital y está asociada a un par de claves pública y privada, generadas en el interior del CHIP del DNI. (Cutanda, 2014).

- Certificado de firma. Certificado utilizado para la firma de documentos garantizando la integridad del documento y el no repudio de origen. Es un certificado X509 v31 estándar, que tiene activo en el Key Usage el bit de ContentCommitment (No Repudio) y está asociada a un par de claves pública y privada, generadas en el interior del CHIP del DNI (Cuerpo Nacional de Policía, 2014).

Es este Certificado expedido como certificado reconocido y creado en un Dispositivo Seguro de Creación de Firma, el que convierte la firma electrónica avanzada en firma electrónica reconocida permitiendo su equiparación legal con la Firma Manuscrita de acuerdo con la Ley 6 (2020) y el Reglamento (UE) Nº 910 (2014).

Carta d'Identità electrónica – Italia

Carta d'Identità Elettronica (CIE) o documento de identidad electrónico italiano, es el documento de identificación personal que se emite desde 2006, únicamente las municipalidades otorgan las CIE a los ciudadanos. Desde el 2016, se están renovando los documentos de identificación tradicional a los documentos de identificación electrónicos el cual incluye un chip que contiene el certificado digital para la autenticación "en línea", y opcionalmente, un certificado para la firma digital.

El CIE es la evolución del carné de identidad en versión papel y consta de un soporte de material plástico de policarbonato, sobre el cual se imprimen con láser la foto y los datos del ciudadano, protegidos con elementos y técnicas antifalsificación, como hologramas y tintas especiales; un microchip sin contacto que contiene:

- Datos personales, Fotografía, Huellas dactilares del titular.
- Esta información se encuentra protegida por mecanismos para evitar su falsificación y/o lectura indebida.

Adicionalmente contiene la información que permite al ciudadano autenticar los servicios en línea prestados por las administraciones públicas y las empresas. En la siguiente imagen se visualiza la cara posterior del documento.

El microchip sin contacto cumple con el estándar de referencia internacional para documentos de viaje electrónicos, como un pasaporte. Incorpora un código numérico que es utilizado por las autoridades supervisoras para leer los datos almacenados en el microchip. Permite leer, decodificar y comprobar la información contenida en el documento de forma automática con herramientas de lectura óptica (OCR).

Características de la Carta d'Identità

En este apartado se describen en detalle los elementos más relevantes que hacen parte del documento electrónico en Italia.

- Código fiscal legible por un escáner óptico. En cada CIE hay un número de serie impreso en el frente en la parte superior derecha y que tiene el siguiente formato: 2 letras - 5 números - 2 letras (por ejemplo, CA00000AA). Este número es el Número Nacional Único.
- El microchip. El microchip sin contacto integrado en el documento convierte al CIE en una herramienta única y segura para verificar la identidad del titular y para acceder a los servicios online de las administraciones públicas y empresas. Los datos personales y biométricos del propietario (fotos y huellas dactilares) se almacenan de forma segura dentro del microchip, así como la información que les permite ser identificados online.

Estos datos, a excepción de las huellas dactilares, pueden ser leídos por el CIE simplemente con una computadora a la que se conecta un lector de tarjetas inteligentes sin contacto o con un

InterSedes, ISSN 2215-2458, Volumen 24, Número 50-
Julio-Diciembre, 2023, pp. 190-224 (Artículo).

teléfono inteligente equipado con una interfaz NFC (Near Field Communication).

El acceso a las huellas dactilares solo está permitido a las autoridades supervisoras con autorizaciones específicas.

- Verificación de la identidad del propietario. Al igual que el pasaporte y el permiso de residencia, el microchip contenido en el CIE cumple con las recomendaciones internacionales de la Organización de Aviación Civil Internacional (2021), en el documento 9303 Documentos de viaje de lectura mecánica en su octava edición que regulan las características de los documentos electrónicos de viaje.
- Símbolo RFID. Esto permite, por ejemplo, utilizar el CIE como documento de viaje reconocido por los países del espacio Schengen. La lectura y verificación de los datos personales y biométricos contenidos en el microchip permite, en los controles por parte del operador, comprobar la autenticidad del documento y la identidad del titular, haciendo más eficientes y seguros los controles policiales.

De acuerdo con las normas internacionales, la lectura de datos personales y fotografías se realiza después de leer una clave de acceso impresa en el documento (CAN - Número de acceso de tarjeta o MRZ - Zona de lectura mecánica). Por lo tanto, un dispositivo no puede leer datos personales sin el conocimiento del propietario.

Documento Nacional de Identidad Electrónico (DNIe) – Perú

Se expidió el DNI-e o DNI electrónico desde el 15 de julio de 2013, dicho documento reemplazó gradualmente al DNI actual. Está disponible para personas mayores de 18 años. Se puede reemplazar cuando el DNI anterior expire y la validez del nuevo documento es de 8 años. El DNI-e peruano, está fabricado en policarbonato y tiene las mismas dimensiones de una tarjeta de crédito, esto de acuerdo con la norma de ISO (the International Organization for Standardization) y IEC (the International Electrotechnical Commission) ISO/IEC 7816-8 (2021). Cuenta

con un chip que se basa en tecnologías de firma electrónica, biometría y tarjeta inteligente. Con el DNI-e las personas naturales pueden firmar digitalmente documentos electrónicos y esto tiene la misma validez que la firma manuscrita, además le permite al ciudadano acceder a diferentes servicios estatales o privados con disponibilidad 24/7, desde cualquier lugar del mundo a través de internet, y cuando en Perú sea implementado, también podrán ejercer el voto electrónico.

Actualmente, el "RENIEC" Registro Nacional de identificación y estado civil emite el Documento Nacional de Identidad (DNI) como un documento público personal e intransferible. Se constituye como la única cédula de identidad personal para todos los efectos civiles, administrativos, comerciales, judiciales y, en general, para todos aquellos casos en que, de acuerdo a lo establecido en la ley, deba ser presentado. Adicionalmente, es el único documento que habilita al ciudadano para ejercer el derecho al voto.

Mediante Resolución Jefatural Número 356 (2005), es aprobado el DNI bajo el formato estándar ISO ID-1 que se utiliza para tarjetas de identificación, cuenta con las siguientes medidas: 8,54 centímetros de ancho por 5,4 de alto en posición horizontal, y se decide que el nuevo documento contenga la misma información, características y los elementos de seguridad que el formato del DNI anterior que estaba bajo el formato ISO ID-2. Es importante tener en cuenta que el cambio del DNI (Formato ISO ID-2) por el nuevo formato (Formato ISO ID-1), no es de carácter obligatorio. Lo que quiere decir que ambos formatos están vigentes.

De acuerdo con el artículo 45° del Reglamento de la Ley de Firmas y Certificados Digitales:

> El Documento Nacional de Identidad electrónico (DNIe) es un Documento Nacional de Identidad, emitido por el Registro Nacional de Identificación y Estado Civil - RENIEC, que acredita presencial y electrónicamente la identidad personal de su titular, permitiendo la firma digital de documentos electrónicos y el ejercicio del voto electrónico presencial… (y) no presencial en los procesos electorales. Ley de Firmas y Certificados Digitales (2000).

InterSedes, ISSN 2215-2458, Volumen 24, Número 50-
Julio-Diciembre, 2023, pp. 190-224 (Artículo).

Características del documento nacional de identidad

A continuación, se detallarán las características de seguridad del formato de DNI más reciente: DNI - FORMATO ISO ID-01, este formato estándar según la norma ISO/IEC 7810 (2019) para las personas a partir de los 17 años. Para la impresión del documento se utiliza la tecnología de Impresión Láser, cuenta con una fotografía a color con trama en la superficie Código único de Identificación y Primer Apellido del titular, así como una fotografía "fantasma" del titular en blanco y negro. Se incluye un código de barras bidimensional PDF417 conteniendo información biométrica de las impresiones dactilares del titular; también, un código de barras lineal Code39 con el Código único de Identificación. Dicho código de acuerdo con la Organización de Aviación Civil Internacional (2021), en el documento 9303 Parte 3, con caracteres OCR-B referidos a los datos del titular. Las fechas de emisión y caducidad del documento.

La lámina Plástica está compuesta de polietileno y poliester para integración molecular con el papel y resistencia al uso, film termosellable, su espesor es de 250 micrones. La impresión es personalizada con el logo de *IDENTIDAD* con 45° de inclinación en dos sentidos, con tinta iridione transparente con efecto OVI, de fluorescencia al amarillo bajo la luz ultravioleta. Finalmente, un marco perimétrico de 2 mm. con bordes redondeados para sellado y protección mecánica.

3.4 Procesamiento de análisis

Con el fin de identificar los componentes y características presentes en cada uno de los modelos que se han seleccionado para el estudio se realiza un cuadro comparativo que permite visualizar de mejor manera la información, elementos técnicos y de seguridad con los que cuenta cada documento. La tabla que se muestra a continuación, permite evidenciar que para cada país se tienen en cuenta diferentes características y datos en el documento, se encuentra que en los casos europeos se omite la impresión de la huella dactilar, toda vez que dicha información está almacenada electrónicamente. Por otra parte, se puede observar que existen

varios atributos que son comunes en todos los casos y otros que no son comunes y solamente se presentan en un solo documento.

Tabla 1

Cuadro comparativo sistemas de identificación

Características	España	Italia	Uruguay	Perú
Chip	X	X	X	X
NFC	X			
Grabado láser	X	X	X	X
CLI	X			X
CLII				X
Características OCR	X	X	X	X
RF		X	X	
Firma Digital	X	X	X	X
Certificados	X	X	X	X
Número de soporte	X			
Número CAN	X			
Código de control		X		X
Código fiscal		X		
Código de barras		X	X	X
Número DNI o identificación	X	X	X	X
Número de registro de nacimiento		X		X
Datos personales (nombres y apellidos)	X	X	X	X
Sexo	X	X		X
Estatura		X		
Fotografía	X	X	X	X
Firma manuscrita	X	X	X	X
Huella impresa			X	X
Fecha de nacimiento	X	X	X	X
Lugar de nacimiento	X	X	X	
Fecha de emisión		X	X	X
Fecha de validez o expiración	X	X	X	X
Expedidor	X	X	X	X
Nacionalidad	X	X	X	
Dirección de domicilio	X			X
Padres	X			
Observaciones			X	
Donante de órganos				X
Estado civil				X
Grupo de votación				X

Fuente: Elaboración Propia

InterSedes, ISSN 2215-2458, Volumen 24, Número 50-Julio-Diciembre, 2023, pp. 190-224 (Artículo).

La gestión de la identidad es de vital importancia para todos los ciudadanos y países. Con el aumento en la cantidad de documentos de identidad electrónica (eID) en circulación a nivel mundial, los diferentes gobiernos han invertido en programas de gestión de identidad para prevenir el fraude y la falsificación y proporcionar a los ciudadanos acceso a una amplia gama de servicios y tecnologías de alta seguridad.

Los datos personales del titular de un documento (ciudadano), incluidos los datos biométricos, deben recopilarse y registrarse correctamente en el chip electrónico del documento. Esto garantizará una identificación de manera rápida y eficaz y una verificación posterior del documento.

La implementación de una cédula electrónica hace que sea casi imposible de falsificar el documento y proteger los datos personales en todas las situaciones que se requiera el uso del documento, ejemplo: emisión de documentos, verificación de documentos al viajar, verificación de identidad, acceso a servicios del gobierno, entre otros.

En cuanto a la interacción de los ciudadanos con aplicaciones y servicios de identificación electrónica adicionales (visa electrónica, gobierno electrónico, firma electrónica, etc.). Permite agilizar y acceder de manera más fácil y eficiente a todos estos servicios. También la implementación de tecnología de credenciales derivadas permitirá a los ciudadanos verificar y autenticarse con su documento a través de un dispositivo móvil.

La norma ISO/IEC 7810 (2019) define en particular, el tamaño habitual de una tarjeta de identificación. El tamaño ID-1 es de 85,60 × 53,98 mm (3 3⁄8 pulg. × 2 1⁄8 pulg.) Y esquinas redondeadas con un radio de 2,88 a 3,48 mm. Este formato se utiliza para PET, PVC, PLA ecológico, policarbonato o incluso tarjetas de metal completo. Se utiliza para identificaciones, licencias de conducir y tarjetas de salud en muchos países. Las dimensiones de la tarjeta de crédito (con o sin chip) son las mismas, con un grosor de 0,03 pulgadas o 0,76 mm.

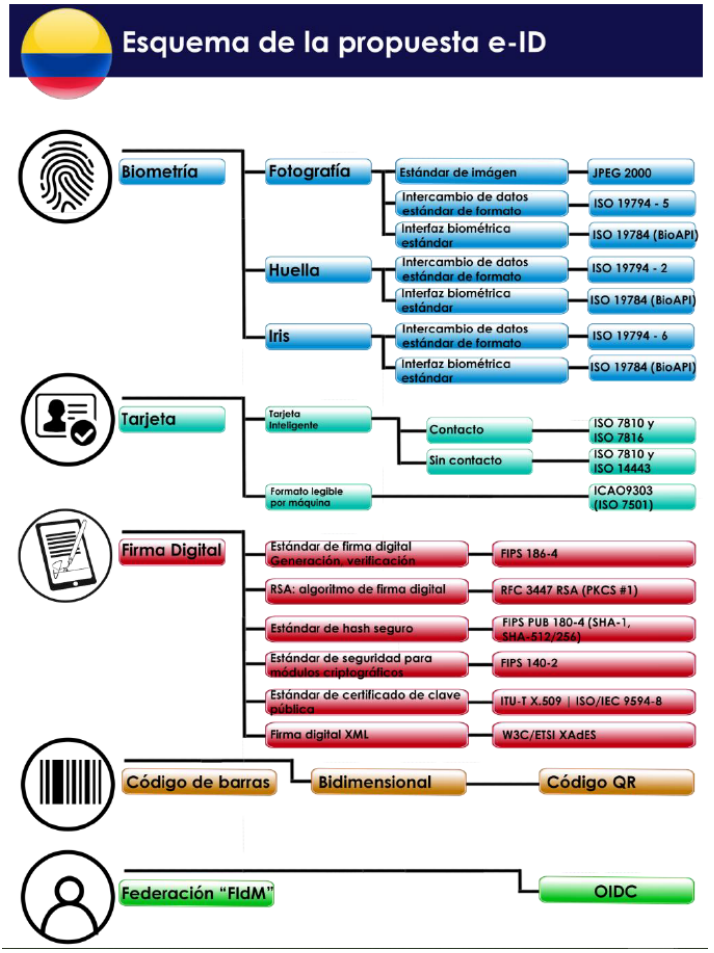
ISO/IEC 7816-8 (2021) es un estándar internacional relacionado con tarjetas de identificación electrónicas con contacto, especialmente tarjetas inteligentes, gestionado conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). ISO/IEC 14443-3 (2011) define el estándar para tarjetas sin contacto.

4. Resultados

En este apartado se realiza una descripción más detallada de la propuesta para la implementación de un sistema de cédula electrónica en Colombia para identificación digital, además de los elementos de seguridad que se consideran deben hacer parte del esquema, como se muestra en la siguiente figura.

Figura 1

Propuesta de la identificación digital para Colombia



Fuente: Elaboración Propia

InterSedes, ISSN 2215-2458, Volumen 24, Número 50-
Julio-Diciembre, 2023, pp. 190-224 (Artículo).

En Colombia la Registraduría Nacional del Estado Civil, es una entidad autónoma con funciones específicas, que incluyen registro civil (nacimiento, matrimonio y defunción) e identificación, dentro del esquema propuesto esta entidad le debe proporcionar a los ciudadanos colombianos una identidad digital, que puede ser autenticada física y virtualmente. La cédula electrónica debe contar con certificados digitales, que le permitan al portador o titular del documento firmar documentos electrónicos. En el presente estudio se toma como referencia a nivel sudamericano el eID de Perú, el cual cumple con la norma ISO/IEC 7816-8 (2021) y su sistema biométrico cumple con el estándar ISO/IEC 19794-4 (2011). Debido a que la tarjeta también se utiliza como un recorrido legible por máquina documento (MRTD), también cumple con lo establecido por la Organización de Aviación Civil Internacional (2021), en el documento 9303 Documentos de viaje de lectura mecánica. Además de esto se considera que se deben contemplar otros aspectos relevantes que se mencionan a continuación:

Biometría. Características físicas únicas, como las huellas dactilares, se pueden utilizar para el reconocimiento automático. En la Registraduría Nacional del Estado Civil, la biometría se utiliza para identificar a los ciudadanos a través del cotejamiento de las huellas dactilares contra el Sistema Automático de Identificación de Huellas Dactilares AFIS.

El AFIS (*Automated Fingerprint Identification System*) es un conjunto de hardware y software especializados que permite el almacenamiento de las imágenes de huellas dactilares, codifica, clasifica y compara automáticamente, para garantizar la identidad de las personas (Innovatrics, 2018). La plataforma AFIS trabaja de forma integrada con la base de datos transaccional MTR.

Fotografía. La impresión de la imagen del rostro del titular en el documento es un elemento fundamental para un reconocimiento efectivo. Es recomendable que dicha imagen sea grabada en el documento a color con técnica de grabado láser en el anverso protegido por un holograma transparente superpuesto a la imagen y en el reverso con técnica "fantasma". Algunas características que

se deben tener en cuenta son las siguientes:

- Dimensiones: las dimensiones de la imagen deben tener una relación de aspecto cuadrada (la altura debe ser igual al ancho). Las dimensiones mínimas aceptables son 600 x 600 píxeles. Las dimensiones máximas aceptables son 1200 x 1200 píxeles.

- Color: la imagen debe estar en color (24 bits por píxel) en el espacio de color sRGB, que es la salida común para la mayoría de las cámaras digitales.

- Formato de archivo: la imagen debe estar en formato de archivo JPEG.

- Tamaño de archivo: la imagen debe ser menor o igual a 240 kB (kilobytes).

- Compresión: Es posible que sea necesario comprimir la imagen para que esté por debajo del tamaño máximo de archivo. La relación de compresión debe ser menor o igual a 20: 1.

- Resolución: 600 dpi

Intercambio de datos formato estándar. A continuación, se realiza una breve descripción del estándar que se considera debe tenerse en cuenta al momento de realizar la implementación de la cédula electrónica en Colombia, toda vez que es fundamental que se cumplan este tipo de requisitos para obtener un sistema de identificación optimo y con calidad.

ISO/IEC 19794-5 (2011). Estándar internacional que especifica los requisitos en cuanto a:

- Escena (fondo e iluminación, posicionamiento, enfoque de la cámara, etc.)

InterSedes, ISSN 2215-2458, Volumen 24, Número 50-
Julio-Diciembre, 2023, pp. 190-224 (Artículo).

- Fotografía (lo que se debe capturar, pose, expresión, etc.)
- Digitalización (calidad de imagen, resolución de imagen, tamaño de imagen, etc.)
- Formato para las imágenes

Huella dactilar. A través de la huella dactilar se permite realizar la comparación en la base de datos (AFIS) con el fin de identificar plenamente al ciudadano, la Metodología de identificación biométrica que utiliza tecnología de imagen digital para obtener, almacenar y analizar datos de huellas dactilares, y que se utiliza dentro del sistema Eurodac: sistema europeo de comparación de impresiones dactilares de los solicitantes de asilo, para el reconocimiento y comprobación automática de huellas dactilares. Reglamento (UE) N°. 603 (2013).

En el esquema planteado se almacena la información biométrica correspondiente a la huella dactilar pero no se imprime en el documento físico, esto debido a que no se considera de utilidad que esta huella sea visible, puesto que el cotejamiento se realiza de manera transparente para el usuario final. Como se ha podido identificar en el análisis sobre la evolución del documento de identidad en Colombia históricamente se ha dispuesto de un espacio en el documento para imprimir la huella del índice derecho, lo cual cambia en el esquema propuesto.

ISO / IEC 19794-4 (2011). La parte 4 de este estándar especifica el formato de intercambio de los registros de datos para el almacenamiento, registro y transmisión de la información de una o más áreas de imágenes de dedos o palmas dentro de una estructura de datos ISO/IEC 19785-1 (2015). Esto puede ser utilizado para intercambiar y comparar los datos de imágenes de dedos. Del mismo modo define el contenido, formato y unidades de medida para el intercambio de datos de imágenes de dedos que pueden ser usados en el proceso de verificación o identificación de un sujeto o ciudadano. La información consta de una

variedad de elementos obligatorios y opcionales, incluidos los parámetros de escaneo, imágenes sin comprimir o comprimidas e información específica del proveedor. Dicha información está destinada al intercambio entre organizaciones que dependen de dispositivos y sistemas automatizados con fines de identificación o verificación basados en la información de las áreas de imágenes de dedos.

Iris. El reconocimiento de iris o escaneo de iris no es más que un proceso que usa luz visible y cercana al infrarrojo para tomar una fotografía de alto contraste del iris de determinada persona. Es una forma de tecnología biométrica ubicada en la misma categoría que el reconocimiento facial y las huellas dactilares. Los expertos investigadores que defienden la tecnología de escaneo de iris afirman que es posible comparar imágenes de iris con una base de datos de imágenes existente para determinar o confirmar la identidad del sujeto. También afirman que los escáneres del iris son más rápidos y fiables que los escáneres de huellas dactilares, ya que resulta más sencillo para un individuo oscurecer o alterar sus dedos que alterar sus ojos. Dentro de las ventajas clave que presenta la tecnología de reconocimiento de iris, se incluyen:

- Velocidad de coincidencia o de cotejamiento.
- Alta precisión.
- Estabilidad de la forma, el color y la textura del iris.

Documento físico. En este apartado se realiza una descripción sobre las características del documento físico, la cual es fabricada en policarbonato, es impresa mediante técnicas que garantizan seguridad ante posibles falsificaciones, alteraciones o manipulaciones. Se propone que el documento integre un chip que cuente con capacidad de almacenamiento y proceso de datos. Las dimensiones corresponderán con el formato ID-1 (85,6 x 53,98 mm) según normativa aplicable ISO/IEC-7810 (2019), ISO/IEC-7816-8 (2021) y ISO/IEC-10373-1 (2020). El documento estará compuesto por un

InterSedes, ISSN 2215-2458, Volumen 24, Número 50-
Julio-Diciembre, 2023, pp. 190-224 (Artículo).

núcleo blanco de policarbonato y varias láminas de policarbonato transparente en anverso y reverso, formando un conjunto con un espesor de 760 micras (+/- 80 micras).

Las credenciales físicas utilizadas para la identificación pueden integrar características de seguridad física y óptica que hacen difícil para los falsificadores crear documentos falsos. En muchos países se utilizan estas medidas de seguridad en sus tarjetas de identificación o para los pasaportes, esto para dotar al documento de elementos anti-falsificación. Las características de seguridad física y óptica que se utilizan comúnmente en la actualidad incluyen las siguientes:

- Holograma: Es un gráfico de apariencia tridimensional creado mediante tecnología láser que se coloca en cualquier lugar de la superficie de la tarjeta antes de la laminación. Cuando los hologramas verdaderos se rompen, cada pieza muestra la imagen original completa, pero desde una perspectiva diferente cada vez que la tarjeta es visto desde un ángulo diferente. Por tanto, los hologramas son difíciles de recrear.

- Imagen fantasma: Es un gráfico semi-visible (en algunos casos se utiliza otra foto del titular del documento) aplicado a la tarjeta. Hologramas o logotipos con imágenes fantasma impresas en combinación con números de identificación son particularmente difíciles de falsificar.

- Microimpresión: Parece una línea delgada ordinaria a simple vista, pero consta de pequeñas imágenes o personajes que tienen menos de 0,3 mm de altura, por lo general solo se pueden leer con una lupa o un microscopio.

- Impresión de arco iris: Esta impresión se utiliza normalmente para disminuir los intentos de falsificación. Esta técnica implica imprimir degradados de varios colores en la superficie de un material a través de un sofisticado proceso de litografía. Cuando se requieran funciones de seguridad

> mejoradas, es posible implementar características de seguridad de tarjetas inteligentes, en el contexto de los sistemas de identidad, el documento de la Organización de Aviación Civil Internacional (2021), en el documento 9303 define muchas opciones de seguridad electrónica disponibles para proteger los datos y los intercambios de datos.

Tarjeta inteligente. Las tarjetas inteligentes cuentan con chips de microprocesador integrados que brindan una capa adicional de seguridad para los usuarios, se parecen en apariencia a una tarjeta de crédito o a una licencia de conducir, pero en lugar de ser una sola pieza de plástico, en realidad están construidas como pequeñas cajas que contienen un microprocesador en sí. Debido a que no utilizan bandas magnéticas como las tarjetas de crédito y débito normales, las tarjetas inteligentes no se pueden leer de la misma manera que las tarjetas normales, estas se leen mediante ranuras físicas destinadas a la lectura de chips o mediante Wi-Fi de corto alcance mediante comunicación de campo cercano o NFC.

Firma Digital. Una firma electrónica se refiere a una firma que se procesa, almacena o transmite electrónicamente. Esto incluye, entre otros, documentos transmitidos electrónicamente con firmas manuscritas, como un documento PDF con firma manuscrita, y documentos digitales que han sido codificados con firma electrónica. Por su parte, las firmas digitales son un subconjunto importante de firmas electrónicas. Las firmas digitales utilizan una técnica conocida como criptografía asimétrica que requiere dos componentes: una clave privada para que el remitente firme un documento y una clave pública para que el receptor la utilice para verificar la firma.

Las claves son generadas por una autoridad de certificación, un tercero de confianza, como una empresa privada o el gobierno. Las autoridades de certificación emiten certificados digitales que contienen estas claves públicas, junto con información sobre los propietarios y los protocolos criptográficos utilizados. El certificado está firmado por la autoridad de certificación emisora y es válido solo para un intervalo de fechas especificado. La clave

InterSedes, ISSN 2215-2458, Volumen 24, Número 50-
Julio-Diciembre, 2023, pp. 190-224 (Artículo).

pública de una autoridad de certificación se distribuye normalmente en paquetes de software, como navegadores web. Una infraestructura de clave pública (PKI) define el conjunto de autoridades de certificación para firmas digitales y las relaciones de confianza entre las distintas autoridades de certificación.

5. Conclusiones

Concluyendo, en Colombia la cédula de ciudadanía tiene tres funciones esenciales:

- Identifica a los ciudadanos colombianos.
- Permite que los ciudadanos puedan ejercer sus derechos civiles.
- Permite la participación por parte de los ciudadanos en la actividad política.

Por otra parte, al implementar la forma de identificación electrónica es posible obtener las siguientes ventajas:

- Un alto nivel de seguridad en el documento de identidad, lo cual dificulta la falsificación.
- Se logran disminuir de manera sustancial casos de suplantación personal y de fraudes.
- Comodidad para el ciudadano, puesto que es viable para personas naturales firmar digitalmente algunos documentos, evitando de esta manera el desplazamiento físicamente.
- Ejercer el voto electrónico de forma remota, esto aplica para países en donde este mecanismo electoral esté vigente y se esté empleado.

- Realizar pagos oficiales en línea (impuestos).

- Acceso a diferentes servicios del orden estatal o privados, 24 horas de día, 365 días del año y adicionalmente desde cualquier parte del mundo.

- Identificarse en Internet, usar la firma electrónica y obtener documentos administrativos online, también cabe la posibilidad de presentar la declaración de impuestos de manera virtual.

La última década, ha representado una evolución en cuanto al intercambio digital de información y masificación de dispositivos y aplicaciones móviles, lo que ha generado que surja una solución que pueda garantizar la identidad del emisor o del receptor, esto en términos de identidad digital. Se han encontrado antecedentes desde el año 1997, en donde desde la fase de diseño, producción y despliegue de tarjetas de identificación electrónicas nacionales seguras han buscado cumplir con ese requisito. De lo cual se obtiene como resultado, el concepto de una tarjeta de identificación válida para los dominios físicos y digitales.

Algunos países que son más visionarios han saltado la identidad móvil o m-ID, lo que representa la creación de un mecanismo, que parte desde el componente de identificación electrónica nacional, para acceder a servicios en línea con un alto nivel de seguridad a través de los dispositivos móviles.

El formato electrónico de estas tarjetas implica que además de utilizarse para aplicaciones de firma electrónica, también son ideales para otros casos de uso, estos pueden incluir conceder al ciudadano acceso a infraestructuras de empresas o ubicaciones seguras e incorporar tarjetas de seguridad social y, en algunos casos, licencias de conducir, tarjetas de atención médica, tarjetas de acceso para servicios de transporte, tarjetas de pago e incluso tarjetas bancarias.

En el caso de Bélgica, la ley que avaló la implementación de la nueva tarjeta de identificación electrónica requirió que el gobierno ofreciera a los ciudadanos una aplicación denominada

InterSedes, ISSN 2215-2458, Volumen 24, Número 50-
Julio-Diciembre, 2023, pp. 190-224 (Artículo).

My File (Embassy of Belgium in the United Kingdom, 2018), que es accesible en línea. Dicha aplicación les permite a las personas saber quién ha accedido a sus datos. Adicionalmente se pone a disposición de los ciudadanos un formulario de consulta o queja, que también puede solicitar que el gobierno justifique cualquier acceso registrado. Lo que planeta una alternativa interesante para la implementación en el país. Ya que con esto se contribuye a tener un alto nivel de transparencia, ya que el ciudadano puede monitorear quien accede a sus registros.

Los estados o naciones que han desplegado este tipo de sistemas de identidad nacional para optimizar los servicios y procesos en los servicios sociales, impuestos, votación y la administración, además de promover los servicios privados estimulando la economía digital, todo esto sucede mientras se reducen los costos para el estado y para el ciudadano.

Las tarjetas inteligentes se reconocen ampliamente como una de las formas más seguras y confiables de identificación electrónica. Con el fin de proporcionar el mayor grado de confianza en la verificación de identidad, la tecnología biométrica se considera esencial en el diseño de un sistema de identificación seguro. La combinación de la tecnología de tarjetas inteligentes con la biometría proporciona los medios para crear una vinculación positiva de la tarjeta inteligente con el titular de la tarjeta, lo que permite una verificación y autenticación sólidas de la identidad del ciudadano.

El uso de e-ID también puede facilitar muchos tipos de servicios de gobierno electrónico. El gobierno puede simplificar muchos servicios, como la prestación de beneficios gubernamentales, que dependen de conocer la identidad de un individuo. El gobierno también puede ofrecer mejores servicios innovadores, como la votación en línea, que requieren autenticación remota.

6. Referencias Bibliográficas

Cuerpo Nacional de Policía. (2014). Características electrónicas de la tarjeta. https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_083

Cutanda, D. (2014). Fundamentos sobre Certificados Digitales – El estándar X.509 y estructura de certificados. https://www.securityartwork.es/2014/04/07/fundamentos-sobre-certificados-digitales-el-estandar-x-509-y-estructura-de-certificados/

Decreto 1010 del 2000. Organización interna de la Registraduría Nacional del Estado Civil. Colombia. 6 de junio del 2000. D.O. No. 46341.

Decreto 1413 de 2017. [Ministerio de Tecnologías de la Información y las Comunicaciones]. Estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales. Colombia. 25 de agosto de 2017.

Decreto 1151 de 2008. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones. Colombia. 14 de abril de 2008.

Directiva 95/46/CE de 1995. [Parlamento Europeo y del Consejo de la Unión Europea] relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Unión Europea. 24 de octubre de 1995.

Embassy of Belgium in the United Kingdom. (2018). My FILE. https://unitedkingdom.diplomatie.belgium.be/en/belgians-uk/my-file

International Organization for Standardization, International Electrotechnical Commission. (2021). Tarjetas de identificación — Tarjetas de circuitos integrados. https://www.iso.org/obp/ui/#iso:std:iso-iec:7816:-8:ed-5:v1:en

Innovatrics. (2018). AFIS (Automated Fingerprint Identification System). https://www.innovatrics.com/glossary/afis-automated-fingerprint-identification-system/

ISO/IEC 7810. (2019). Identification cards — Physical characteristics. https://www.iso.org/standard/70483.html

ISO/IEC 7816-8. (2021). Identification cards — Integrated circuit cards — Part 8: Commands and mechanisms for security operations. https://www.iso.org/obp/ui/#iso:std:iso-iec:7816:-8:ed-5:v1:en

ISO/IEC-10373-1 (2020). Cards and security devices for personal

identification — Test methods — Part 1: General characteristics. https://www.iso.org/standard/70482.html

ISO/IEC 14443-3. (2011). Identification cards — Contactless integrated circuit cards — Proximity cards — Part 3: Initialization and anticollision. https://www.iso.org/standard/50942.html

ISO/IEC 19785-1. (2015). Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification. https://www.iso.org/standard/66179.html

ISO/IEC 19794-4. (2011). Information technology — Biometric data interchange formats — Part 4: Finger image data. https://www.iso.org/standard/50866.html

ISO/IEC 19794-5. (2011). Information technology — Biometric data interchange formats — Part 5: Face image data. https://www.iso.org/standard/50867.html

ISO/IEC 19794-7. (2014). Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data. https://www.iso.org/standard/55938.html

Ley 39 de 1961. [Congreso de la República]. Por la cual se dictan normas para la cedulación, y otras de carácter electoral. Colombia. 18 de julio de 1961. D.O. No. 30572.

Ley 6 de 2020. Reguladora de determinados aspectos de los servicios electrónicos de confianza. España. 11 de noviembre del 2000.

Ley 27269 de 2000. Ley de Firmas y Certificados Digitales. Perú. 26 de mayo de 2000

Lozada, D. (2020). ¿Cómo combatir la suplantación y la falsedad documental? https://www.infolaft.com/como-combatir-la-suplantacion-y-la-falsedad-documental/

Ministerio de las Tecnologías de la información y las Comunicaciones (2018). Política de Gobierno Digital. https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/

Organización de Aviación Civil Internacional. (2021). Doc 9303 - Documentos de viaje de lectura mecánica. Octava edición. https://www.icao.int/publications/Documents/9303_p1_cons_es.pdf

Organización de Aviación Civil Internacional. (2021). Doc 9303 - Documentos de viaje de lectura mecánica. Octava edición.

Parte 3: Especificaciones comunes a todos los MRTD. https://www.icao.int/publications/Documents/9303_p3_cons_es.pdf

Registraduría Nacional del Estado Civil. (2012). El Registro Civil, base de la identificación. https://www.registraduria.gov.co/1-de-octubre-de-2012-No-68-El.html#:~:text=El%20Nuip%20es%20un%20n%C3%BAmero,edad%20y%20la%20c%C3%A9dula%20de

Reglamento (UE) No. 603 de 2013. [El Parlamento Europeo y el Consejo de la Unión Europea]. relativo a «Eurodac»: la base de datos dactiloscópicos de los solicitantes de asilo de la Unión Europea para comparar sus impresiones dactilares. Unión Europea. 26 de junio de 2013.

Reglamento (UE) No. 910 de 2014. [El Parlamento Europeo y el Consejo de la Unión Europea]. relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. Unión Europea. 23 de julio de 2014.

Resolución Jefatural Número 356 de 2005. Mediante la cual es aprobado el DNI bajo el formato estándar ISO ID-1. Perú. 15 de marzo de 2005.

Sánchez, S. (2016). Gestión de Identidad en las Administraciones Públicas: Interoperabilidad pan-europea. https://docplayer.es/613742-Gestion-de-identidad-en-las-administraciones-publicas-interoperabilidad-pan-europea.html