UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIOLOGÍA

MÁSTER EN GOBIERNO Y ADMINISTRACIÓN PÚBLICA

TRABAJO FIN DE MÁSTER

CURSO 2022 – 2023

ANÁLISIS DE LA COMPLEJIDAD CONCEPTUAL Y TÉCNICA DE LA IDENTIDAD DIGITAL EN ESPAÑA

Iria Moreno Rodriguez

Docente al cargo:

Luis Antonio Martínez Gómez

Junio 2023

Resumen

El presente estudio tiene como propósito el análisis del desajuste entre el nivel de oferta de servicios públicos digitales y el nivel de uso que hace la ciudadanía de estos. Como parte del analisis se tratará de determinar si dicho "gap" es atribuible a la complejidad de los mecanismos de identidad digital existentes en España y aportar soluciones en base al análisis comparado de identidades digitales del ámbito europeo.

Abstract

The purpose of this study is to analyse the mismatch between the level of digital public services on offer and the level of use of these services by citizens. As part of the analysis, we will try to determine whether this gap is attributable to the complexity of the existing digital identity mechanisms in Spain and to provide solutions based on a comparative analysis of digital identities in Europe.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN

El tema que se va a analizar en el presente trabajo se centra en el estudio de la interacción *ad extra*[1] entre la ciudadanía y la Administración Pública a través de medios digitales.

De acuerdo con las investigaciones relativas a la administración pública y a la identidad digital en España, se describe la existencia de un desajuste entre la oferta de servicios públicos digitales y los niveles de demanda de dichos servicios digitalizados.

Lo que se pretende pues, es analizar dicho desajuste - entre oferta y demanda de servicios públicos digitales- y analizar si este fuese atribuible – y en qué medida - a la identidad digital, ya que esta, de entrada, no presenta un buen nivel de desarrollo en comparación[2] con otros elementos de digitalización.

Con lo previo nos vendríamos a preguntar ¿Por qué si la Administración Pública en España presenta tan alta digitalización se da un nivel de uso comparativamente inferior? ¿Qué papel juega ahí la denominada identidad digital?

Es decir, si los productos y servicios a los que se pretende acceder se encuentran disponibles en formato digital, ¿Por qué no se usa en la misma medida? ¿Sería debido al deficiente nivel de desarrollo de la identidad digital en España?

Por lo que se refiere a las motivaciones para llevar a cabo la presente investigación, destaca mi motivación personal y académica. Como cualquier otro ciudadano, derivado del acontecimiento cotidianos, he tenido que interactuar con la Administración Pública por medios electrónicos, por ende, mediante el uso de los mecanismos de identificación electrónica, esto sin haber tenido una experiencia plenamente satisfactoria.

[1] Alude a las relaciones entre la Administración Pública y sus administrados (empresas y ciudadanos) diferenciándose de las relaciones «ad intra» las cuales hacen referencia a la manera en la funciona de manera interna cada Administración y las relaciones entre ellas.
[2] Vid Tabla 1. Resumen de puntuación en materia de digitalización de la Administración Pública española (2022)

Lo previo, junto con mi interés académico por la digitalización de la Administración Pública, me ha motivado a analizar la problemática identificada.

1.1 Objetivos

Por lo que respecta a los objetivos generales que guían la presente investigación, nos centraremos en analizar el impacto de la identidad digital en las relaciones entre la Administración Pública y los ciudadanos por medios electrónicos, identificando las principales características de la administración digital, asi como entrando al detalle de la identidad digital. Por último, se llevará a cabo un analisis comparativo de identidades digitales en el ámbito europeo.

En base al analisis comparativo, se plantea el objetivo específico de establecer líneas de mejora en base a las barreras identificadas.

1.2 Hipótesis

La hipótesis principal con la que se trabaja en la presente investigación es que la identidad digital – y su complejidad técnica - es una de las principales responsables del desajuste identificado entre la oferta de servicios públicos digitales y el uso que los ciudadanos hacen de ellos.

Es decir, que el desajuste entre oferta y demanda es atribuible a la identidad digital en España.

1.3 Espacio y período

Para responder a las preguntas que fundamentan el presente trabajo, se plantea un estudio con las limitaciones temporales y espaciales expuestas a continuación.

Por lo que respecta a las limitaciones espaciales, el caso de estudio se acota a la Administración Pública española y a las relaciones *ad extra* entre administración y ciudadano. Complementariamente, a partir de una perspectiva comparada, se estudiará el funcionamiento de los mecanismos de identificación electrónica y firma digital contemplados en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP)

Asimismo, puesto que se pretende hacer uso del análisis comparativo para analizar los modos de hacer en otros países, se abrirá el foco pudiéndose llegar a contemplar países de ámbito europeo.

El periodo de analisis es el periodo actual, entiendo este como el periodo comprendido entre 2016 – fecha más temporada de la cual existen bases de datos al respecto del caso de estudio – hasta mayo del 2023. Con la horquilla seleccionada se busca contextualizar la situación actual de la identidad digital española y tener cierta sensibilidad sobre la evolución que ha experimentado.

Por último, el analisis se complementará con una breve revisión histórica referente a la transformación digital desde la década de los 70 en adelante en el territorio español.

1.4 Estructura

Para el análisis de lo expuesto previamente, se propone una estructura que se desarrollará del siguiente modo:

- Se detallará lo que entendemos por identidad digital, asi como la situación de la identidad digital en España. Esto se complementará mediante un analisis comparado con el nivel de desarrollo de las identidades digitales en otros países (principalmente del ámbito europeo).
- Se describirá analíticamente la complejidad de la identidad digital partiendo de la premisa de que la introducción de un nuevo modelo de relación con la Administración Pública ya es compleja en sí.
- Es base a la descripción analítica de los diferentes mecanismos de interacción con la Administración Pública se categorizarán los elementos que dada su complejidad puedan suponer una barrera al uso de la Administración digital.
- Se finalizará con el analisis de los modos de hacer de otros países en materia de identificación electrónica con los que perceptiblemente pudiesen superarse las barreras identificadas previamente.

2 METODOLOGIA

Para responder a las preguntas planteadas se hará uso de una metodologia descriptiva, analítica y cuantitativa para evidenciar la complejidad en los mecanismos de identificación electrónica y firma digital en el caso español.

En la línea se hará un analisis descriptivo analítico de algunos aspectos contemplados en la LPACAP que regula las relaciones entre la Administración Pública y ciudadanos por medios electrónicos.

De la misma se extrae el enunciado de cuáles son los mecanismos[3] de identificación electrónica y firma digital sobre las cuales vamos a trabajar – sistema cl@ve, certificado digital y DNI electrónico – así como las distinciones funcionales entre los actos de identificación electrónica y firma digital.

Complementariamente se accederá a los sitios web oficiales – o de las autoridades competentes - respectivos de cada mecanismo y se procederá a hacer una analisis descriptivo analítico a partir del cual caracterizar la complejidad de estos.

Dicho analisis se hará mediante el desgranamiento de cada uno de los mecanismos, asi como de las diferentes etapas del proceso hasta completarlo.

El análisis se complementará con la perspectiva aportada por diagramas de flujos[4] de elaboración propia, a partir de la cual se esquematizará el proceso de registro, puesta en marcha y uso de los diferentes mecanismos de identidad digital.

Los diagramas constan de elementos que indican el inicio y fin del trámite (elipse), elementos que indican proceso (rectángulo redondeado), elemento de indican que existen alternativas (rombo), asi como elementos que indican que un proceso debe continuarse en una página web externa (pentágono). Tambien se contemplan cuadros aclaratorios (rectángulo con borde granate), asi como

[3] Se excluyen del análisis las soluciones de identificación electrónica y firma digital autonómicas

[4] Estos se utilizan, entre otras cosas, para comunicar procesos complejos en diagramas claros y fáciles de comprender (Lucidchart)

iconos que informan sobre los docuemntos a aportar. Por último, las flechas de flujo.

Una vez se haya realizado la descripción y analisis exhaustivo previo, se identificarán y categorizarán los elementos de complejidad observados. Dichos elementos de complejidad se distinguen entre los que podemos considerar complejos en sí, dado su alto carácter técnico, y otros elementos que no se consideran complejos en sí, pero complejizan el proceso.

Todos ellos se categorizarán y codificarán – para su rapida identificación – en categorias de complejidad conceptual, técnica, informacional y procedimental para cada uno de los mecanismos – sistema cl@ve, certificado digital y DNIe -.

Una vez respondida la hipótesis principal, se llevará a cabo un analisis comparado para identificar de qué modo otros modelos de identidad digital han superados las barreras identificadas en el caso español.

3 ESTADO DE LA DIGITALIZACIÓN EN ESPAÑA

La finalidad del presente capitulo será la de definir cuál es la situación actual de España en materia de digitalización(oferta) y penetración social(demanda), es decir, la efectividad de las medidas emprendidas por el gobierno en materia digital, en comparación con los niveles de uso de la administración digital por parte de los ciudadanos.

Para entender el posicionamiento actual de España en lo que respecta a la digitalización de la Administración Pública debemos remontarnos a principios de los años 70 y más intensamente en a finales de esta, con la propuesta de la Comisión al Consejo de inclusión de la política de telecomunicaciones como materia de ámbito comunitario y la decisión de llevar a cabo la transformación de la Administración tributaria a mediados de los años 80 (Casarrubios, 2020) junto con las subsecuentes medidas llevadas a cabo hasta la actualidad[5]

Dichas medidas y/o planes ejecutados a lo largo de las décadas[6], reflejan los óptimos niveles de digitalización de la Administración Pública y *overperformance*[7] en algunos ámbitos.

El estado actualizado de la digitalización de la Administración Pública se puede consultar en múltiples informes llevados a cabo por instituciones de alto reconocimiento como las Naciones Unidas, la Organización para la Cooperación y el Desarrollo Económico (OCDE) u otras como la Comisión Europea. Consecuentemente, encontramos múltiples informes y/o bibliografía sobre el histórico de evolución y la situación actual de la administración española[8]

[5] Véase (Arenilla, 2021) La Administración Digital pg 184 - 200
[6] Véase: Repensando la Administración Pública (2021) Tabla 1. Evolución del marco político-estratégico de Administración digital en España
[7] Véase: eGovernment Benchmark 2022. Background Report pg.92
[8] Recopilación de informes respectivos al estado de las administraciones en terminos de digitalización en el Portal de Administración Electrónica. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_OBSAE/Posicionamiento-Internacional/Resumen-posicionamiento-Espana.html

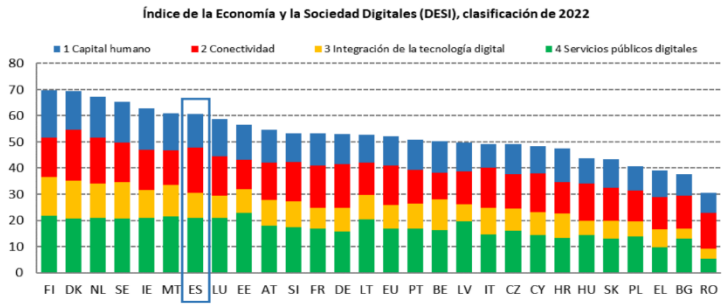
En terminos generales, de acuerdo con los informes observados, la Administración Pública española presenta unos índices de desarrollo óptimos[9], resultados que a continuación desgranaremos.

Por lo que respecta a informes emitidos por la Comisión europea – la cual incluye el estudio de administraciones pertenecientes a la Unión Europea – destaca el Índice de Economía y sociedad digital (DESI)[10] en el cual, España se encuentra en la séptima posición de entre los 27 países analizados, con una puntuación del 60,8 lo cual supone unos 8,5 puntos por encima de la media de la UE.

En concreto se encuentra entre de Malta y Luxemburgo con puntuaciones de 60,9 y 58,9, respectivamente.

Figura 1.

Índice de la Economía y la Sociedad Digitales (2022)



Fuente: Tomado del Índice de la Economía y la Sociedad Digitales (DESI) 2022 España

Dicho informe se nutre de cuatro ámbitos de análisis entre los cuales encontramos el análisis del «capital humano», de la «conectividad», de la «integración de la tecnología digital» y por último los «servicios públicos digitales», siendo esta última categoría la que presenta mejor puntuación.

[9] Así se evidencia en el eGovernment Benchmark 2022. *Background Report* (Comisión Europea, 2022, pg. 92), informe en el cual, en material de digitalización la Administración Pública española se encuentra *On-track* – un nivel de desarrollo adecuado para su coyuntura y potencial – en algunos aspectos y *Over-performing* – presenta niveles de desarrollo por encima de su óptimo - en algunos otros.

[10] El Índice de Economía y Sociedad Digital (DESI) clasifica a los países de estudio según el nivel de digitalización de los países, así como los avances en terminos de Capital Humano, Conectividad, Integración de la tecnología digital y Servicios públicos digitales.

Podemos asumir que por lo que respecta a la digitalización de servicios públicos, la Administración Pública española presenta una puntación notable en comparación con el resto de los ámbitos de estudio.

En este caso y dado que el presente estudio se centra en el analisis de la digitalización en la Administración Pública, mostraremos especial atención al índice que parametriza este mismo ámbito - la situacion de los servicios públicos digitales en la Administración Pública española -.

En dicho índice, España se encuentra en quinta posición dentro del entorno europeo. En este caso tambien presentando una puntuación superior a la de la media europea.

Este se configura en base a la parametrización de 4 elementos: (1) usuarios de la administración electrónica - a partir del cual se hace referencia al nivel de interacción digital entre la Administración Pública los ciudadanos y empresas - en el cual España obtiene una puntuación del 73%, 6 puntos porcentuales superior al mismo índice pero para la media de la UE (2) formularios precumplimentados, indicador que alude al cuestiones de interoperabilidad, es decir, el nivel de reutilización de la información que se transmiten de unas administraciones a otras a fin de facilitar los trámites a los ciudadanos (Portal de Administración Electrónica, 2023), (3) Servicios públicos digitales para ciudadanos y Servicios públicos digitales para negocios en el que España presenta puntuaciones del 87% y 94%, respectivamente, y por último, (4) Datos abiertos en el que se obtiene una puntuación del 95%.

Figura 2.

Resumen posicionamiento España en servicios públicos digitales

	España			UE
	DESI 2020	DESI 2021	DESI 2022	DESI 2022
4a1 Usuarios de la administración electrónica % usuarios de internet	63 % 2019	67 % 2020	73 % 2021	65 % 2021
4a2 Formularios precumplimentados Puntuación (0 a 100)	NP	NP	78 2021	64 2021
4a3 Servicios públicos digitales para los ciudadanos Puntuación (0 a 100)	NP	NP	87 2021	75 2021
4a4 Servicios públicos digitales para empresas Puntuación (0 a 100)	NP	NP	94 2021	82 2021
4a5 Datos abiertos % puntuación máxima	NP	NP	95 % 2021	81 % 2021

Fuente: Tomado del Índice de la Economía y la Sociedad Digitales (DESI) 2022 España

Tal y como se observa en la figura 2, la Administración Pública española presenta una evaluación favorable - en aquellos indicadores existen datos - asi como mejores puntuaciones en todos los indicadores en comparación con la media de la Unión Europea para el mismo año (2022).

A destacar que, son los indicadores que aluden a la penetración social (usuarios de la administración electrónica) e interoperabilidad (formularios precumplimentados) los indicadores en los cuales se obtienen puntuaciones más bajas.

La misma Comisión Europea tambien ha llevado a cabo los informes *e-Government Benchmark*[11]*.* En terminos generales, España presenta un buen posicionamiento con una puntación de 79 sobre 100 y superando la media europea por 8 puntos. Asimismo, posicionándose por detrás de los líderes en digitalización administrativa como Malta (95%), Estonia (90%), Luxemburgo (87%) o los Países Bajos (85%).

En este aspecto vemos como España destaca por encima de países colindantes de características parecidas como lo son Francia o Portugal con 70% y 78% respectivamente.

Las categorias de indicadores utilizados para evaluar el desempeño digital de las diferentes administraciones son (1) Centralidad del usuario, (2) Transparencia, (3) Habilitadores clave y (4) Servicios transfronterizos. A continuación, se exponen algunos aspectos destacables de dichos indicadores.

En la categoría «centralidad del usuario» - tal y como se puede observar en la tabla 1 - se contemplan los subindicadores de 1.1 Disponibilidad online, 1.2 *Mobile friendliness* y 1.3 Soporte al usuario. Esta categoría es en la que se obtiene una puntuación más elevada - 98 puntos sobre 100 –.

Con esto vemos materializado el intenso esfuerzo de la Administración Pública por digitalizar la prestación de los servicios públicos, esto sí, al peso, es decir se

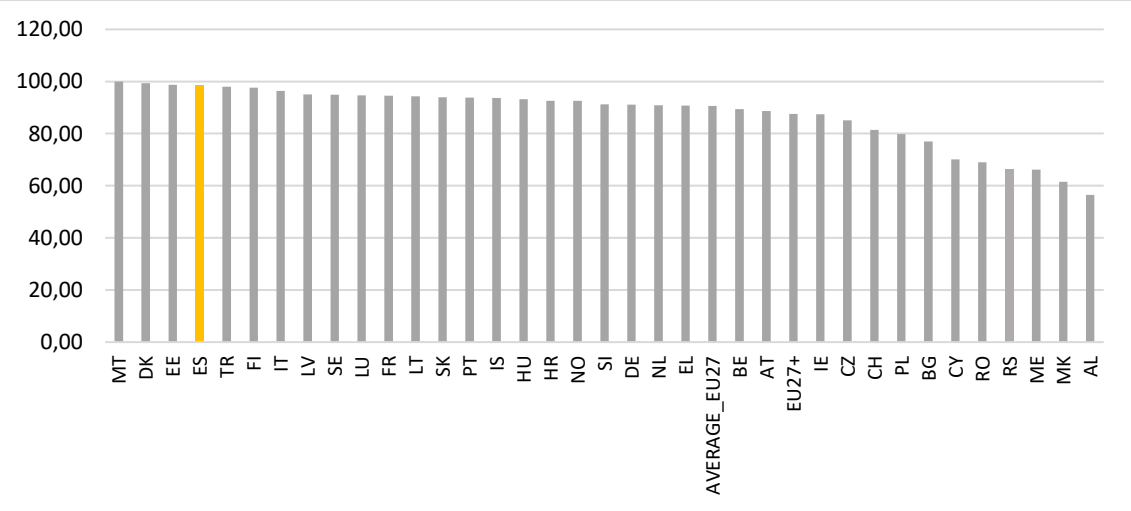
[11] Los informes e-Government Benchmark se tratan de una serie de informes que lleva realizándose desde 2012 y que tienen como objetivo comparar como los gobiernos de Europa prestan los servicios públicos digitales (Comisión Europea, 2022)

ve como cerca del 100% de servicios se han digitalizado y el 90% de ellos tambien los encontramos soportados por dispositivos móviles.

En terminos comparativos, tal y como observamos en la figura 3 vemos como la Administración Pública española obtiene un excelente posicionamiento, solo por detrás de Malta, Dinamarca y Estonia lideres digitales indiscutibles.

Figura 3.

Nivel de disponibilidad online - «online availability» de servicio públicos



Fuente: Elaboración propia a partir del eGovernment Benchmark (2022)

En segundo lugar, por puntuación obtenida, observamos que en la categoría de «habilitadores clave» se presenta una puntuación de 77,9 sobre el total.

De esta categoria se puede pensar a simple vista que presenta una buena puntuación, asimismo, si se observan las puntuaciones de los subindicadores pertinentes encontramos la categoría *e-Id*[12] *- identidad digital* -, se obtiene una de las peores puntuaciones, un 53,7. A través de la presente tabla se refleja el deficiente nivel de desarrollo de la identidad digital en España, en comparación con el resto de los indicadores en los cuales se observa un mejor nivel de desempeño.

[12] En el informe analizado eID hace referencia a “identificación electrónica es una solución emitida por el gobierno para la identificación y autenticación en línea” (Comisión europea, 2021) y que, a la vez, aportan mayor seguridad, rapidez y facilidad de accesos a los servicios digitales del gobierno, disuadiendo a los ciudadanos de tener que acudir presencialmente para la realización de determinados tramites (Comisión Europea, 2021)

Dicha puntuación – un 53,7 – es el reflejo de carencias en el desarrollo que podrían impactar en el nivel de uso que hace la ciudadanía de estos y que, consecuentemente, fomentarían el desajuste entre oferta y demanda de servicios públicos digitales identificado en el analisis y que podremos observar a través de la comparación entre los datos de las figuras 3 y 4 de este mismo capítulo.

Tabla 1.

Resumen de puntuación en materia de digitalización de la Administración Pública española (2022)

Puntuación del país		Promedio bienal 2020 + 2021	Eventos de la vida empresarial 2020 + 2021	Eventos de la vida ciudadana 2020 + 2021	Promedio (2021)
ES	**0. Puntuación global**	**78,8**	**84,3**	**77,3**	**79,0**
ES	1. Centralidad del usuario	95,5	97,3	95,0	98,0
ES	1.1 Disponibilidad online	95,3	96,3	95,1	98,5
ES	1.2 Mobile friendliness	90,4	97,8	88,3	90,7
ES	1.3 Soporte al usuario	98,4	100,0	98,0	100,0
ES	2. Transparencia	72,4	72,1	72,5	73,0
ES	2.1 Transparencia en la prestación	63,9	84,4	58,0	60,1
ES	2.2 Transparencia de los datos personales	83,9	69,3	88,0	88,8
ES	2.3 Transparencia del diseño del servicio	69,4	62,5	71,4	70,0
ES	3. Habilitadores clave	79,1	86,5	76,9	77,9
ES	3.1 eID	59,7	62,2	59,0	53,7
ES	3.2 Documentos electrónicos	84,7	93,8	82,2	87,9
ES	3.3 Fuentes auténticas	78,2	90,0	74,3	82,3
ES	3.4 Correo digital	94,4	100,0	92,9	90,0
ES	4.Servicios transfronterizos	68,5	81,4	64,7	67,1
ES	4.1 Disponibilidad transfronteriza en línea	81,7	91,0	79,0	78,7
ES	4.2 Soporte al usuario transfronterizo	74,1	100,0	66,7	86,7
ES	4.3 Servicios transfronterizos	13,7	11,8	14,3	8,2
ES	4.4 Documentos electrónicos transfronterizos	58,9	75,7	54,1	40,8

Fuente: Tomado del eGovernment Benchmark (2022)

Complementariamente, en la tabla que se muestra a continuación, tabla 2, podremos observar que, una vez más, la identidad digital sale mal parada con una de las peores evoluciones a lo largo del periodo 2016-2021. A diferencia del resto de indicadores en el nivel de desarrollo de la identidad digital incluso presenta datos regresivos.

Esto previo, contrasta con una evolución favorable observable en el resto de los indicadores. El foco de digitalización se ve en la categoria de «centralidad del usuario» en la cual se observa una mejora unánime y una puntuación del 98% en 2021. Destacan la excelente *performance* por lo que respecta a la disponibilidad online, accesibilidad a través de dispositivos móviles «*Mobile friendliness*» o el apoyo al usuario en la web «soporte al usuario».

En este sentido, podemos concluir que en terminos de oferta de servicios públicos digitales, se observa un excelente desempeño.

Tabla 2.

Evolución de la digitalización en España

	Promedio (2021)	Promedio (2020)	Promedio (2019)	Promedio (2018)	Promedio (2017)	Promedio (2016)
0. PUNTUACIÓN GENERAL	**79,0**	**78,7**	**76,9**	**78,9**	**69,1**	**77,2**
1. Centralidad del usuario	98,0	92,4	98,0	89,3	93,7	87,8
1.1 Disponibilidad online	98,5	91,4	99,8	91,7	97,5	92,5
1.2 Mobile friendliness	90,7	90,1	82,7	53,7	57,9	35,6
1.3 Soporte al usuario	100,0	96,4	100,0	100,0	100,0	100,0
2. Transparencia	73,0	71,7	76,2	77,9	67,6	78,4
2.1 Transparencia de la prestación de servicios	60,1	68,6	62,2	78,7	54,0	79,5
2.2 Transparencia de los datos personales	88,8	77,7	83,0	62,3	72,0	63,3
2.3 Transparencia del diseño del servicio	70,0	68,8	.	.	.	.
3. Habilitadores clave	77,9	80,5	78,5	80,9	68,8	77,1
3.1 eID	53,7	67,2	59,8	78,2	44,4	76,7
3.2 Documentos electrónicos	87,9	80,8	98,8	79,7	99,5	82,1
3.3 Fuentes auténticas	82,3	74,2	83,3	78,0	67,8	74,6
3.4 Correo digital	90,0	100,0	75,0	87,5	62,5	75,0
4. Servicios transfronterizos	67,1	70,1	55,0	59,5	46,5	59,6
4.1 Disponibilidad transfronteriza en línea	78,7	85,5	64,3	55,6	57,7	73,0
4.2 Soporte al usuario transfronterizo	86,7	58,3	75,0	83,3	58,3	50,0
4.3 Servicios transfronterizos	8,2	20,6	2,5	13,6	0,0	11,1
4.4 Documentos electrónicos transfronterizos	40,8	81,6	40,0	73,5	33,3	73,3

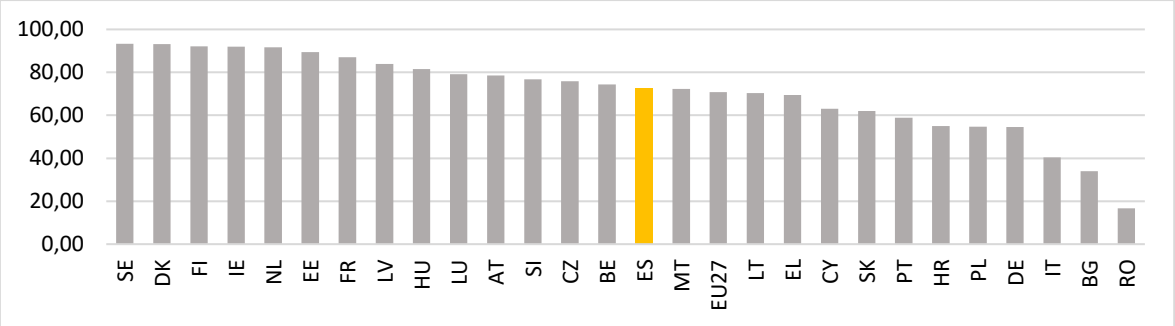
Fuente: Tomado del eGovernment Benchmark España (2016-2021)

En contraposición a los niveles de digitalización – las medidas emprendidas por los gobiernos en materia digital - encontramos los niveles de penetración social de los servicios públicos digitales – la respuesta ciudadana a dichas medidas.

En este sentido vemos como España no obtiene un posicionamiento tan notable sino que, en este caso, se encuentra en la decimoquinta posición, con una puntuación de 72,2%. Aun así, por encima de la media europea.

Figura 4.

Nivel de penetración social Unión Europea (2022)



Fuente: Tomado del eGovernment Benchmark (2022)

Llegados a este punto, si comparamos los niveles y posicionamiento internacional de la Administración Pública española en los niveles de oferta de servicios públicos digitales y los niveles de uso de los mismos, vemos como se constata el desajuste entre ambos parametros. Dicho desajuste no es puntual sino que se trata de un desajuste histórico (Criado, 2021)

La existencia de dicho desajuste – observable a través de los informes analizados - asi como por bibliografia previamente revisada, nos da a entender que existen algunas ineficiencias que lo generan y lo sustentan en el tiempo. En el presente estudio se trabajará sobre la hipótesis de que parte de dicho gap es atribuible a la identidad digital, identificada como «*eID*» en los informes mostrados previamente.

A fin de determinar el nivel de implicación de la identidad digital en el desajuste persistente entre oferta de servicios públicos digitales y demanda de los mismos, se llevará a cabo un analisis descriptivo en la que se parametrizará la complejidad de los mecanismos de identidad digital en España.

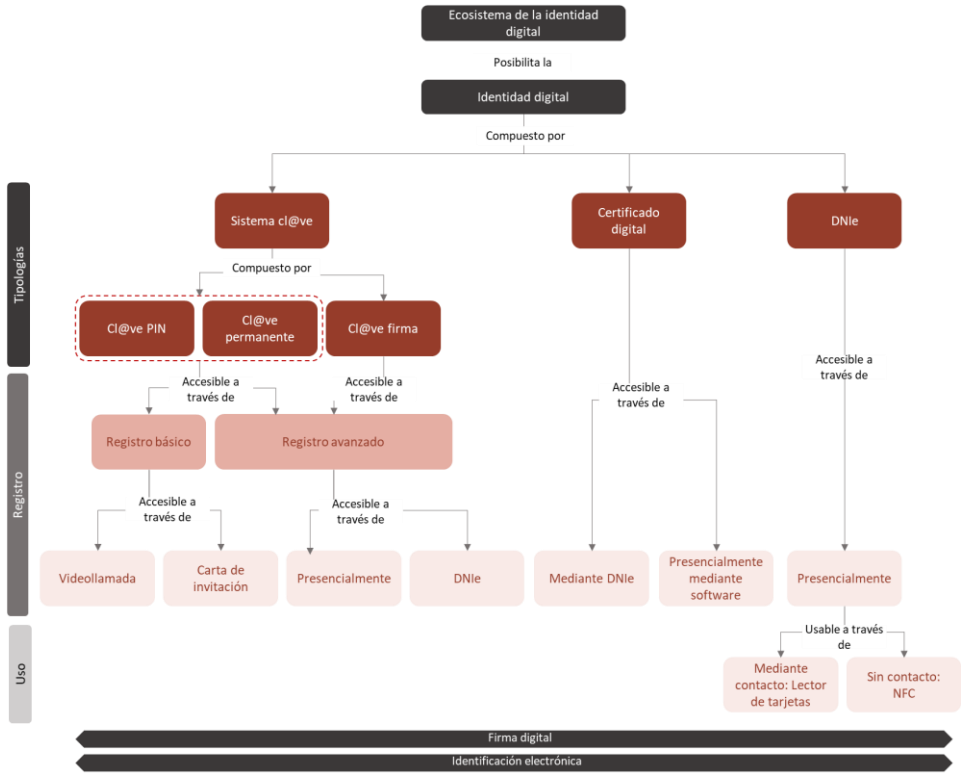
4 LA IDENTIDAD DIGITAL EN ESPAÑA

La finalidad del siguiente capítulo será analizar la complejidad técnica de los mecanismos de identidad digital en España, así como la exposición de las diferencias entre el proceso de «identificación tradicional» y el proceso de «identificación electrónica», entre los actos de «identificación electrónica» y «firma digital» y las diferencias entre los mecanismos desarrollados para interactuar con la administración pública – sistema cl@ve, certificado digital y DNI electrónico -.

Los diferentes mecanismos se analizarán siguiendo el itinerario "idílico"[13] que perceptiblemente seguiría el interesado hasta poder hacer uso de los mecanismos de identidad digital tal y como se muestra en la figura 5.

Figura 5.

Esquema del ecosistema de la identidad digital en España



Fuente: Elaboración propia a partir de los datos de la investigación

[13] Itinerario que deduciblemente un ciudadano seguiría a fin de obtener un mecanismo de interacción con la Administración Pública. En este caso se entiende la (1) comprensión del ecosistema de mecanismos disponibles (2) el registro en el mecanismo de conveniencia (3) la puesta en marcha y (4) su uso.

Lo previo, con la pretensión de entender detalladamente cada uno de los mecanismos, las diferencias entre ellos, que actos posibilitan, asi como los modos y procederes para su obtención.

4.1 Ecosistema conceptual de la identidad digital

La identidad y la gestión de esta son imprescindibles para el acceso e interacción con el mundo digital, en este caso con la Administración Pública digital (Bernal, 2022, pg. 295; Criado, 2021) y razón de éxito de las administraciones digitales (Arenilla, 2021, pg. 143)

Asimismo, en el presente capítulo nos preguntamos de qué modo los gobiernos han «traducido» la identidad al mundo digital. ¿Cómo se traslada algo tan básico como la auto evidencia del yo, al mundo digital?

La identidad, tradicionalmente la entendemos como la relación entre una entidad – física o jurídica – y un conjunto de datos de identificación, como podrían ser el nombre, apellido, lugar de nacimiento, etcétera (Bernal, 2022, pg. 295-300)

Dicho de otro modo, la identidad hace referencia al conjunto de rasgos que caracterizan a una persona frente a las demás, permitiéndole interactuar con su entorno y constituyéndose en base a las condiciones propias de cada persona y sus propias experiencias (Martínez y Rincón, 2021, pg. 253). Tal y como se expone en la figura 6, esta se hace valer a través de un proceso llamado identificación, en el cual se exhibe ante un tercero un documento que vincula a la entidad con un conjunto de datos/rasgos característicos. Un ejemplo de dichos documentos disponibles en soporte físico son el Documento Nacional de Identidad o el Pasaporte en su defecto.

Asimismo, “con base en este nuevo panorama tecnológico, y en la gran cantidad de datos existentes que se encuentran en línea para realizar diferentes transacciones y operaciones en internet, es necesario identificarse y conocer quién es la persona que está realizando la respectiva transacción en la red” (Martínez y Rincón, 2021, pg. 252). Consecuentemente, ha sido necesaria la conceptualización de la identidad en el mundo de lo digital, como se comentaba previamente, ha sido necesaria la «traducción» de la identidad tradicional al mundo digital.

La «identidad digital», de igual modo que la «identidad tradicional» y cómo podemos observar en la figura 6, hace referencia a un conjunto de rasgos que hacen referencia a una entidad física o jurídica y permite a los individuos su identificación, reconocimiento e individualización en ámbitos como el digital (Martínez y Rincón, 2021, pg. 255).

Dicha identidad digital se ve sujeta a marcos regulatorios que preservan derechos, regulan transacciones o intentan la prevención de delitos (Martínez y Rincón, 2021, pg. 256) y se materializa a través servicios, plataformas, elementos hardware y software que permiten identificar y autentificar a los interesados, es decir les permite tener un reconocimiento en el mundo digital (Martínez y Rincón, 2021, pg. 256)

Dada las características del canal digital, la identificación no se puede llevar a cabo a través de la exhibición de un documento verificador de la identidad, sino que tenemos que valernos de mecanismos de identificación electrónicos para tal hecho.

El proceso de identificación electrónica se trata del «proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica» (art. 3.1 del Reglamento eIDAS)

Es decir, la «identificación electrónica» se trata de un proceso que nos permite autenticar la identidad de una entidad – física o jurídica – pero en este caso a través de medios electrónicos (Bernal, 2022, pg.300)

Orbitando en torno al concepto de identificación, y qué, frecuentemente se confunde, encontramos el conceto de «autentificación», este, a diferencia de la identificación hace referencia a un proceso de verificación en general (Ortega, s.f.) o tal y como se recoge en el apartado 5 del reglamento eIDAS, la autentificación hace referencia a un «proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico»

Por tanto, tal y como apunta Domingo (2018, pg.44) la autentificación se trata de un concepto más amplio, al contemplar, no solo las funciones de la identificación

- autentificación de la identidad de entidades - sino que tambien contempla la autentificación de otros elementos.

Fruto de las diferencias entre identificación y autentificación y las implicaciones derivadas, en la LPACAP 39/2015, es la que por primera vez se establecen y regulan diferentes mecanismos dependiendo de si su función es la autentificación de la identidad (identificación) o la autentificación de la voluntad y el consentimiento expresos (firma digital).

Es decir, vemos que se identifican y regulan de manera diferenciada los «Sistemas de identificación de los interesados en el procedimiento», los cuales permiten autenticar la identidad de entidades y los «Sistemas de firma admitidos por las Administraciones Públicas», los cuales permiten «acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento» (art.10. Ley 39/2015).

Por un lado, tendriamos los mecanismos que habilita la ley para la identificación electrónica de entidades:

- Los «certificados electrónicos cualificados de firma electrónica» y los «certificados electrónicos cualificados de sello electrónico».

- «Cualquier otro sistema que las Administraciones públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital»

En este caso, los principales mecanismos de identificación electrónica a disposición de la ciudadanía que cuentan con estas características serían el sistema cl@ve - cl@ve PIN y cl@ve permanente – el certificado digital de la Fábrica Nacional de Moneda y Timbre (en adelante FNMT) y el DNIe.

Complementariamente, como se venía comentando, tambien se contemplan los mecanismos de firma digital, los cuales, de acuerdo con el art. 10 de la misma ley nos encontramos con:

- Sistemas de firma electrónica cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.
- Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico expedidos por prestador incluido en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.
- Cualquier otro sistema que las Administraciones públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Esta comunicación vendrá acompañada de una declaración responsable de que se cumple con todos los requisitos establecidos en la normativa vigente. De forma previa a la eficacia jurídica del sistema, habrán de transcurrir dos meses desde dicha comunicación, durante los cuales el órgano estatal competente por motivos de seguridad pública podrá acudir a la vía jurisdiccional, previo informe vinculante de la Secretaría de Estado de Seguridad, que deberá emitir en el plazo de diez días desde su solicitud.

Algunos de los comúnmente utilizados son el DNIe, el certificado digital de la FNMT, asi como el mecanismo cl@ve firma.

Más allá de la diferenciación funcional entre los diferentes mecanismos de identidad digital – mecanismos de identificación electrónica y mecanismos de firma digital - la diferenciación regulatoria se fundamenta en base a los principios de «minimización de datos[14]» y «proporcionalidad[15]».

Esto es, “en función del concreto tipo de operación que desee realizarse por medios electrónicos, se necesitará mostrar la identidad o, además, autenticar la

[14] Véase: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a

[15] Véase: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

voluntad: siempre será necesario identificarse; no siempre lo será, en cambio, expresar la propia voluntad" (Bernal, 2022, pg. 305)

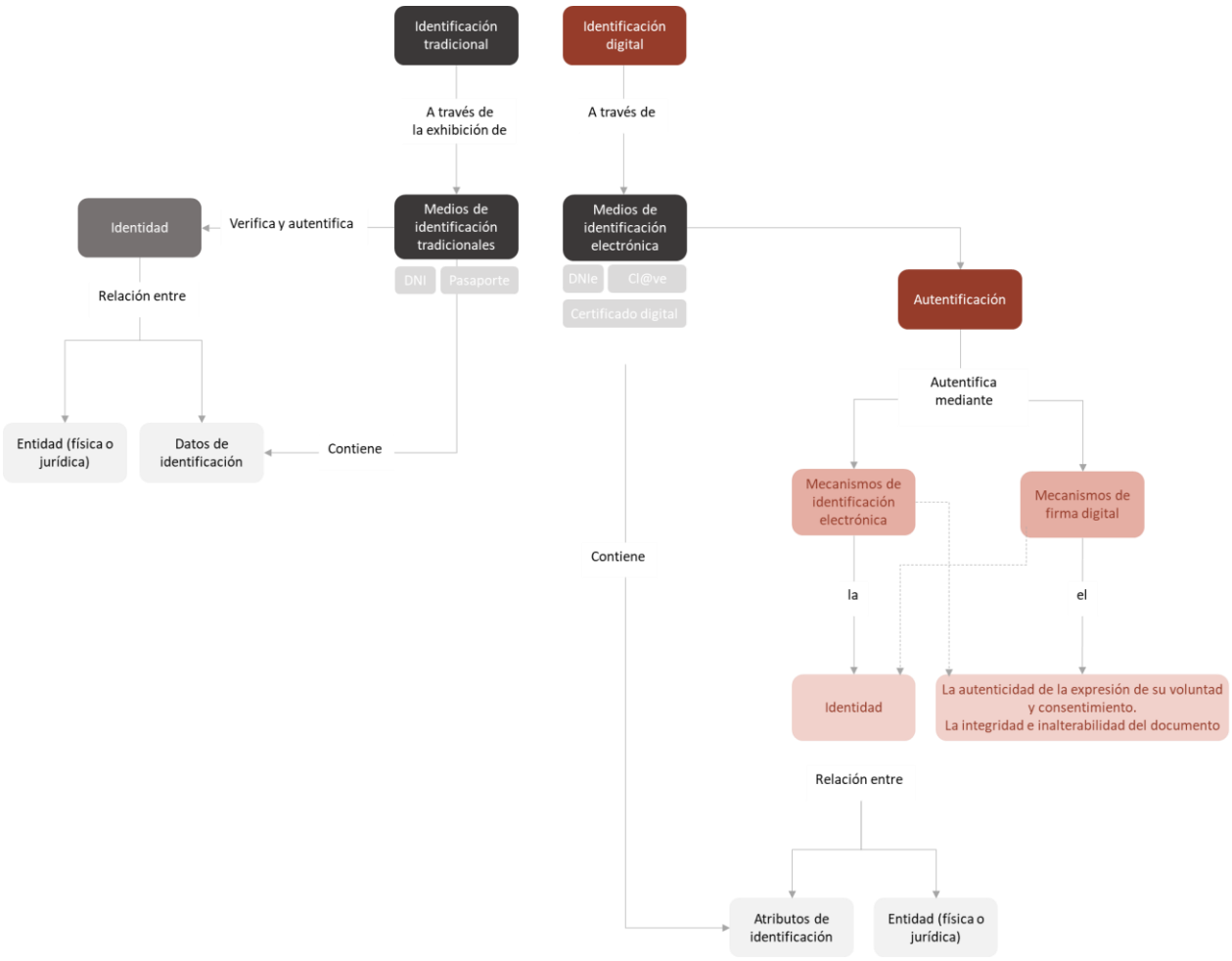
Y asi lo hace constar en el art. 11 de la misma ley "con carácter general, para la sustanciación de las actuaciones previstas en el procedimiento administrativo bastará con acreditar la identidad, requiriéndose la firma sólo para: formular solicitudes, presentar declaraciones responsables o comunicaciones, interponer recursos, desistir de acciones y renunciar a derechos"

Dicha voluntad de diferenciación se ve menoscabada dado qué en el art. 10.3 de la LPACAP establece que, "cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación contemplados en el apartado 2 de dicho precepto como sistema de firma, cuando permitan acreditar la autenticidad de la expresión de la voluntad y el consentimiento de los interesados" (Bernal, 2022, pg. 206) y "en el apartado 4 de ese artículo 10 de la Ley 39/2015, establece expresamente que, cuando los interesados utilicen un sistema de firma de los regulados por la Ley su identidad se entenderá ya acreditada mediante el propio acto de la firma". Por ende, pudiendo utilizar los mecanismos de identificación como firma digital y los de firma digital como mecanismos de identificación electrónica, quedando difusa la distinción entre las funcionalidades y limitaciones de unos y otros.

Todo este conjunto de especificaciones conceptuales y técnicas que diferencian a ambas, «identidad tradicional» e «identidad digital», quedan esquematizadas en el siguiente esquema.

Figura 6.

Esquema de la «Identificación tradicional» e «identificación digital»



Fuente: Elaboración propia a partir de los datos de la investigación

Como podemos observar, ambas identidades - la tradicional y la digital - deben ser autentificadas, asimismo, se observa como en el caso de la identidad digital se ven involucrados otros aspectos como la distinción entre los actos de identificación electrónica y firma digital, asi como de los mecanismos habilitados para lo mismo.

En el caso de la identidad tradicional nos valemos de un documento físico que se encarga de autenticar nuestra identidad y nos valemos de nuestra firma manuscrita para mostrar voluntad y consentimiento explicito.

En el caso de la identidad digital, por el contrario, para identificarnos o firmar digitalmente se tendrían que obtener los mecanismos de identificación necesarios para el trámite que se quiera llevar a cabo. Como veremos, no todos

los mecanismos disponibles sirven para la tramitación de todos los tramites disponibles en formato digital.

4.2 ¿Qué y dónde?: Mecanismos de interacción con la Administración Pública por medios electrónicos

Como se comentaba en el capítulo previo, en España existen diversos mecanismos de identificación y firma digital reconocidos en la LPACAP, concretados en los artículos 9 y 10 de la misma.

Asimismo, en esta se alude a mecanismos genéricos que cumplen con determinadas características y/o “Cualquier otro sistema que las Administraciones públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital” (art. 9 – 10 ley 39/2015). Consecuentemente, y ante la incapacidad de abordar todos los mecanismos potenciales, en el presente trabajo nos centraremos en:

- El sistema cl@ve, gestionado por la Agencia tributaria.
- El certificado electrónico emitido por la FNMT-CRM
- El DNI electrónico emitido por la Dirección General de tráfico (Ministerio de Interior)

Del analisis en profundidad se excluyen las soluciones de identidad digital autonómicas como:

- idCAT Certificado e idCAT Móvil en Cataluña
- Ch@ve 365 en Galicia

- Bak/BakQ o la tarjeta virtual en el País Vasco

Figura 7.

Soluciones de identidad digital en España

	Qué es	Proceso para obtenerlo	Capacidad de gestión	
Cl@ve PIN	DNI/NIE + contraseña de un solo uso	Registro Avanzado: - Presencialmente con DNI/NIE - Online mediante DNIe o certificado Registro Básico - Mediante carta de invitación - Mediante videollamada	Medio	Nacional
Cl@ve permanente	DNI/NIE + contraseña		Registro avanzado: Alta Registro básico: Media	Nacional
DNIe	Certificados insertado en soporte físico (DNI)	- Presencialmente en comisaria	Alta	Nacional
Certificado digital	Certificado digital que se descarga en el ordenador	- Presencialmente con DNI/NIE - Mediante DNIe	Alta	Nacional
idCAT Certificado	Certificado digital que se descarga en el ordenador	- Por internet con Certificado Digital o DNIe - Presencialmente con DNI o NIE	Alta	Regional
idCAT Móvil	Usuario + contraseña de un solo uso	- Por video identificación. Nivel de seguridad media - Con DNI, NIE o TIE + la Tarjeta Sanitaria o de MUFACE. Nivel de seguridad bajo	Media	Regional
Bak	DNI/NIE+ contraseña	Online, mediante formulario de solicitud (pide datos personales y la declaración de la renta)	Bajo	Regional
BakQ	DNI/NIE + CONTRASEÑA + código enviado por SMS	-Presencialmente con DNI/NIE Online, si tiene DNIe o Certificado Digital	Alta	Nacional
Tarjeta virtual	Certificado digital que se descarga en el ordenador	Se puede solicitar online una vez se está registrado en BakQ	Alta	Nacional
ch@ve 365	NIF + contraseña + código de un solo uso que se solicita en cada trámite	- Presencialmente: con cita previa y documentación oficial de identificación - Digitalmente: con DNIe o Certificado digital	Alta	Regional

Fuente: Elaboración propia a partir de los datos de la investigación

A fin de caracterizarlos los seleccionados:

- Se expondrán las principales características de los diferentes mecanismos de identidad digital.
- Se analizará el lugar – sitios web - en el que se detalla la información necesaria para que los interesados puedan registrarse de manera efectiva y obtener los mecanismos de identificación electrónica y firma digital.

4.2.1 Sistema Cl@ve

El sistema cl@ve dice estar orientado a unificar[16] – dado que permite la identificación y firma – y simplificar el acceso electrónico a la Administración

[16] Asimismo, se expone que, actualmente el sistema cl@ve complementa otros sistemas de identificación y firma como el DNI-e y el certificado electrónico.

Pública – al tratarse de un sistema de claves concertadas (usuario + contraseñas) -.

Tal y como expone en el propio sitio web de cl@ve, este se trata de un sistema interoperable y horizontal que evita que las diferentes administraciones tengan que implementar y gestionar sus propios sistemas de identificación y firma, y a los ciudadanos, tener que utilizar diferentes identificaciones electrónicas para relacionarse con la administración.

El sistema clave, permite el acceso a los trámites electrónicos a través de dos vías, (1) a través de una contraseña permanente o (2) un código temporal, vías que se materializan en los mecanismos de identificación: Cl@ve permanente y clave PIN, respectivamente.

- **Cl@ve permanente:** Se trata de un sistema de autentificación de la identidad de seguridad media, pudiéndose elevar mediante la verificación del código numérico de un solo uso o *One Time Password* en inglés (en adelante OTP). Consecuentemente, en determinados trámites será suficiente con introducir el usuario y la clave del interesado y en otros supuestos, que por seguridad se requiera, tambien se tendría que aportar el OTP enviado al dispositivo móvil del interesado.

- **Clave PIN:** De igual modo que la cl@ve permanente, se trata de un sistema de autentificación de la identidad del interesado a la hora de realizar trámites electrónicos con la Administración Pública.
  A diferencia del sistema Cl@ve permanente, el sistema clave PIN, se basa en el uso de un código elegido por el usuario y PIN enviado al teléfono del interesado a través de:
  - la aplicación móvil desarrollada para tales efectos – «clave PIN» -.
  - a través de SMS.

En la línea se observa de acuerdo con un estudio de Prodigioso Volcán apunta a que, aunque el sistema Cl@ve dice estar creado para unificar los sistemas de autentificación, en la práctica su alcance es inferior al del Certificado digital o el DNIe. “No hay ningun trámite de los analizados que se haga con cl@ve que no se pueda hacer con Certificado digital/DNIe, pero sí hay trámites que se hacen con Certificado Digital y DNIe que no se pueden hacer con Clave” (Prodigioso Volcán, 2022, pg. 62)

Dicho PIN tiene una validez limitada en el tiempo y se renovará con cada trámite al que quiera accederse.

En este caso las principales diferencias entre ambos sistemas serían:

- La validez – en terminos de tiempo - de las credencias otorgadas por ambos sistemas
- Los mecanismos de validación – usuario + clave en el caso de la cl@ve permanente y usuario y PIN en el caso de cl@ve PIN – utilizados para validar la identidad del interesado.
- El nivel de seguridad proporcionado por cada uno de los sistemas, siendo cl@ve permanente un mecanismo que aporta más seguridad y consecuentemente mayores credenciales de acceso.

Asimismo, más allá de servicios de identificación electrónica, el sistema cl@ve tambien contempla mecanismos de firma digital.

Recientemente, el sistema Cl@ve ha adquirido la posibilidad de realizar firma electrónica mediante certificados electrónicos centralizados a través del llamado sistema de Cl@ve *firma* “en aquellos tramites en que la firma mediante certificados electrónicos sea requerida o admitida”

4.2.2 Certificado digital de la FNMT-RCM

Del conjunto de certificaciones digitales gestionadas por la FNMT, nos centraremos en aquella habilitada para personas físicas. Esta, de acuerdo con lo expuesto en el sitio web de la Real Casa de la Moneda – FNMT, “vincula a su suscriptor con unos datos de verificación de firma y confirma su identidad”, por ende, este a su vez certifica la integridad del documento y el origen de los datos asi como la identidad del propio interesado, garantizando en todo momento que solo el interesado-ciudadano y su interlocutor – la Administración Pública - pueden acceder a la información que se está intercambiando entre ambos.

Igual que el resto de los mecanismos de certificación electrónica, es un documento electrónico – manifiesto a través de un software - expedido por una autoridad de certificación e identifica a una persona - física o jurídica - con un par de claves (Portal de Administración electrónica, 2023).

El caso del certificado electrónico del ciudadano es uno de los más controvertidos pues cuenta con múltiples nombres, lo cual dificultaría la identificación inequívoca del mecanismo. De acuerdo con las fuentes revisadas se han contabilizado cinco denominaciones[17]. Esto, si asumimos que un ciudadano concreto tiene voluntad de obtener el certificado digital por fuerza externa – se le requiere para realizar un trámite de obligatoria tramitación electrónica –, no identificar de manera clara, sencilla el mecanismo que debe obtener podría generar inseguridad, malestar o frustración.

4.2.3 DNI electrónico

El DNIe – documento análogo al DNI físico - asi como el resto de los mecanismos de certificación electrónica, se expiden por una autoridad de certificación, y tal como se exponía previamente, identifica a una persona con un par de claves que tienen como objetivo validar y certificar que una firma electrónica se corresponde con una persona o entidad concreta (Portal de Administración electrónica, 2023)

Se trata de un certificado digital sostenido sobre soporte físico, el cual es emitido por la Dirección General de Policía (Ministerio del Interior)

Este se trata de un mecanismo, no solo de verificación de la identidad del portador – identificación electrónica – sino que tambien autentifica la voluntad y consentimiento expreso del firmante asi como la integridad del documento– firma digital – permitiendo, no solo autentificar los datos de la identidad del ciudadano sino vincular estos a un documento mediante la firma.

Para lo mismo se vale de dos tipos de certificados que alberga en un pequeño circuito integrado (chip):

- Certificado de Autentificación: Se certifica la identidad del ciudadano al realizar la transacción electrónica (PAe, 2023)
- Certificado de Firma: Es la substituta de la firma manuscrita, por ende, garantiza la identidad del suscriptor y del poseedor de la clave privada de identificación y firma (PAe, 2023)

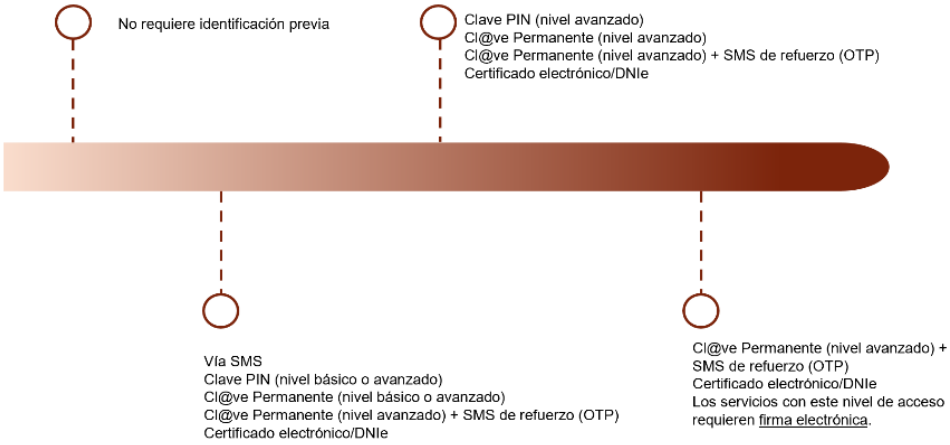
[17] Entre otras, «Certificado de Ciudadano», «Certificado de Usuario» o «Certificado de persona física».

Del conjunto de mecanismos expuestos – sistema cl@ve, certificado digital y DNI electrónico – aquellos aspectos principales que los diferencian son:

- Si se tratan de mecanismos de identificación electrónica, firma digital o ambos.
- Tal y como vemos en la figura 8, los diferentes niveles de seguridad otorgados por cada uno y, consecuentemente, las credenciales para acceder a los diferentes trámites.

Figura 8.

Niveles de seguridad de acceso a los servicios públicos digitales



Fuente: Tomado del informe ¿Son claros los trámites digitales? (2022)

No obstante, dichas diferencias pueden no ser tan claras a efectos prácticos y es que tal y como se ha comentado previamente, en los artículos 10.3 y 10.4 de la LPACAP se dispone la posibilidad de utilizar los mecanismos de identificación para firmar digitalmente y viceversa.

Derivada de dicha difusa distinción funcional, el ciudadano no es capaz de determinar para que utilizar cada mecanismo, y es que, generalmente, las administraciones habilitan la posibilidad de utilizar múltiples mecanismos para un mismo trámite. Asi se evidencia en *¿Son claros los trámites digitales?* (2022, pg.62) donde, se observa que la mayoría de las Administraciones garantizan diversos métodos de acceso a los trámites. Lo que es más es que casi todos los

trámites (62,5%) admiten al menos cuatro formas de identificación y solo el algunos (10%) admiten solo uno.

Perceptiblemente, podría parecer un dato favorable – el hecho de que múltiples trámites admitan una amplia diversidad de sistemas de identificación electrónica - asi mismo, se observan “incongruencias” que podrían generar problemas de desinformación e inseguridad asociados a la aparente aleatoriedad en el uso de estos.

- En el primero de los casos vemos como, existen determinados trámites a los cuales se puede acceder con un sistema de identificación intermedia pero no con todos los sistemas de identificación superior.
- El segundo de los casos de en situaciones se da cuando existen trámites a los que se puede acceder con un sistema de identificación de un determinado nivel, pero no con otros sistemas del mismo nivel de seguridad

A esto le tenemos que sumar la potestad y libertad de las diferentes administraciones para determinar que mecanismo de interacción sería necesario para un determinado trámite. Tal y como apunta Bernal (2022, pg.308) la elección del medio de identificación admisible en cada procedimiento corresponde a cada Administración.

Complementariamente al analisis de los mecanismos en sí, se analiza la ubicación de las fuentes de información relativas a los mecanismos de identidad digital.

De esto cabe destacar dos aspectos, la pluralidad de fuentes y la pluralidad de accesos a la mismas.

Estos cuentan con portales propios. Asimismo, tambien se observan ulteriores sitios web en los que del mismo modo tambien encontramos información al respecto. En terminos generales se observa como las fuentes de información son diversas – ampliamente diversas – incongruentes, desactualizadas, la terminología utilizada no es homogénea y la información en ellos contenida se encuentra en mayor o menor medida desarrollada. Derivado de la existencia de multiplicidad de fuentes gestionadas por distintas entidades, los esfuerzos por mantenerlas actualizadas podrían suponer un mayor esfuerzo.

Complementariamente, los puntos de acceso son diversos, en este caso, podriamos encontrar la información en la propia web de la administración, un chatbot, los textos del propio trámite de interés, listados con preguntas frecuentes, dentro de trámites, pero en enlaces externos o normativas y protocolos adjuntos en un PDF no siempre accesible *(¿Son claros los trámites digitales?*, 2022, pg. 74)

De igual modo, el interesado puede acceder a la información entrando directamente a la web de la Administración en concreto y hacer una búsqueda en ella, hacer una búsqueda en el navegador, entrar a una sede electrónica y guiarse por sus menús y submenús, llamar por telefono al que ofrezcan información al respecto, dejarse guiar por un chatbot, accediendo a la web oficial de los mecanismos de identificación electrónica y firma digital y navegar por los paneles (*¿Son claros los trámites digitales?*, 2022, pg. 74)

4.3 Obtención de los mecanismos de identidad disponibles[18]

En la presente línea de investigación nos centramos en el estudio de los diferentes procesos de obtención de los mecanismos de identificación electrónica y firma digital, asi como en los diferentes modos de registro contemplados para cada uno de ellos.

En este caso, la existencia de más de un mecanismo identificación electrónica/firma digital – como veremos a continuación - implica casi de manera directa la necesidad de más información sobre las diferentes formas de obtención de sendos mecanismos, asi como la diversidad de opciones o alternativas planteadas para cada uno de ellos.

4.3.1 Sistema de identificación Cl@ve: Cl@ve permanente, Clave PIN

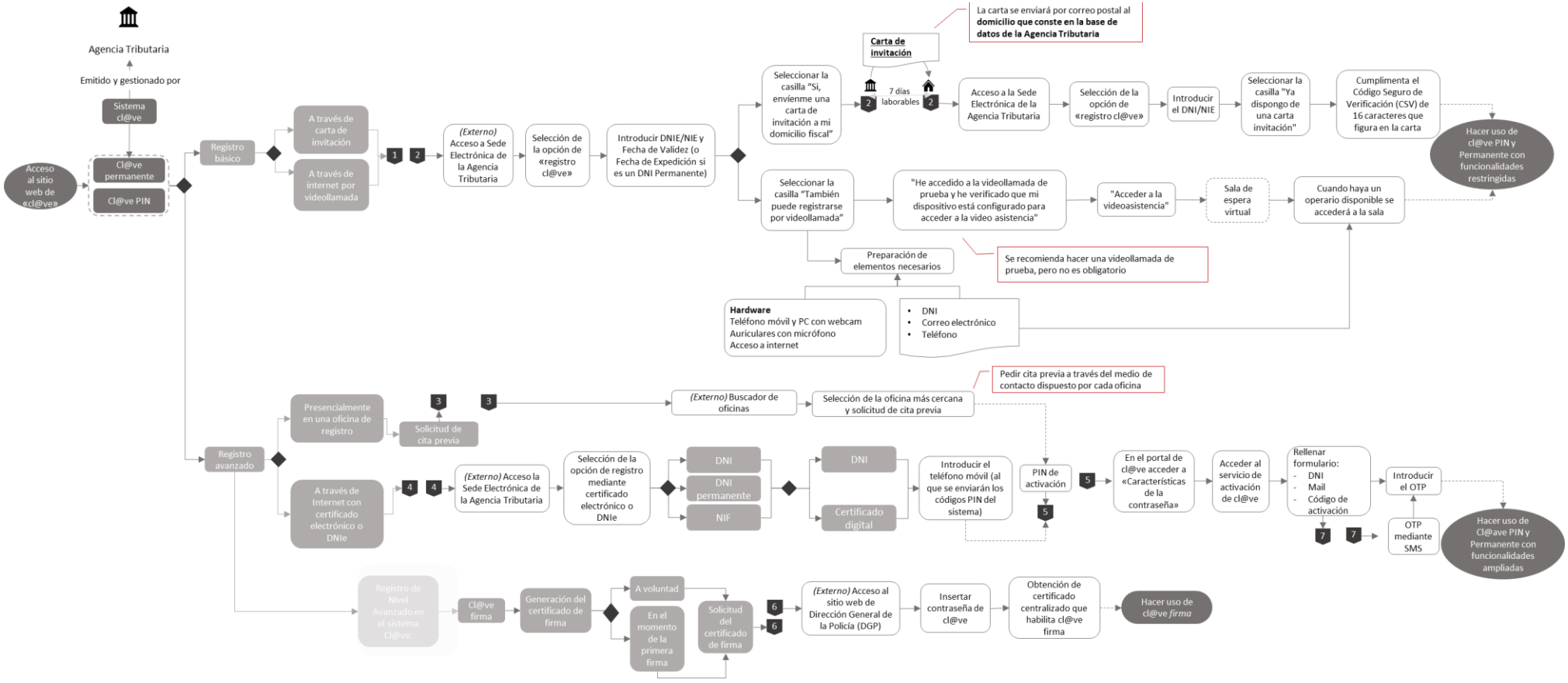
Por lo que respecta a los mecanismos de identificación del sistema Cl@ve, se contemplan los sistemas Cl@ve permanente y cl@ve PIN, los cuales presentan

[18] Los mecanismos de identificación electrónica contemplados en la *LPACAP*

un proceso de obtención conjunta, es decir la obtención de uno implica la obtención del otro. Asimismo, para la obtención de ambos sistemas, es mandatorio el registro previo en el sistema Cl@ve. Proceso contemplado en la figura 9 que se muestra a continuación.

Figura 9.

Diagrama de flujos del itinerario de registro en sistema cl@ve



Fuente: Elaboración propia a partir de sitio web de «cl@ve»

Para dicho registro se habilitan cuatro modalidades comprendidas en dos categorias – registro básico y registro avanzado - y la elección de uno otro modo determinará el nivel de seguridad de las claves obtenidas.

En el caso de que quiera obtenerse a través de un «registro avanzado» el interesado deberá hacerlo (1) presencialmente en una oficina de registro o bien (2) a través de internet mediante el certificado electrónico o DNIe. Procesos que podemos observar en la parte inferior del diagrama.

En el caso de querer realizarlo a través del «registro básico» se pueden obtener los mecanismos de cl@ve a través de (3) carta de invitación o (4) a través de videollamada por el canal online tal y como se observar en la parte superior de la figura 9.

El registro por uno u otro canal determinará el nivel de credenciales otorgadas. En este caso el registro avanzado nos otorgará mayores licencias que los registros básicos y, por ende, acceso a mayor número de trámites.

Asimismo, tal y como podemos observar por el número de pasos y requerimientos un «registro básico» no implica menor complejidad ni menor esfuerzo en terminos de recursos que un «registro avanzado»

4.3.1.1 Registro Avanzado

- Presencial a través de una Oficina de registro

De acuerdo con lo expuesto en el sitio web del sistema Cl@ve para el registro avanzado presencial será imprescindible la personación del interesado asi como la aportación de DNI en vigor para su identificación en las Oficinas de Registro[19] correspondientes. De estas, debería considerarse la capilaridad[20] de las mismas, asi como los plazos medios de espera para la cita deseada.

[19] Funcionan como oficinas de registro distribuidas por toda España la red de oficinas de la Agencia Estatal de Administración Tributaria, de las Entidades Gestoras y Servicios Comunes de la Seguridad Social, del Servicio Público de Empleo Estatal y la red de oficinas de Información y Atención al Ciudadano de las Delegaciones y subdelegaciones del Gobierno (Gobierno de España, 2023) Asimismo, tanto las Comunidades Autónomas como Entidades Locales han habilitado Oficinas de Registro.

[20] No todas las oficinas del buscador gestionan tramites del sistema cl@ve

Al respecto de las citas previas, tal y como se observa en el diagrama, el usuario deberá acceder a un sitio web externo. Complementariamente, dicho buscador no se trata de un buscador exclusivo de oficinas para el registro en cl@ve, sino que se tiene que marcar específicamente que el trámite que quiere llevar a cabo está vinculado con el sistema cl@ve, de lo contrario este dispone un listado genérico de oficinas de la administración pública que no necesariamente gestionan registros de cl@ve. Este buscador es meramente informativo, es decir, no se permite al usuario realizar la solicitud de cita previa a través de dicha interfaz, sino que, se tiene que realizar a través de los datos de contacto proporcionados – correo o telefono – o en algunos casos, a través de ulteriores canales.

En el caso de realizarse la reserva por medio de telefónico[21], se solicitará al interesado el número de identidad y se le enviará mediante SMS un mensaje confirmando la cita y detallando la Oficina y la hora a la que deberá acudirse.

- A través de internet con certificado electrónico o DNI-e

Para el registro mediante certificado o DNIe deben cumplirse cuatro pasos entre los cuales encontramos:

1. La identificación del interesado mediante la introducción de los datos requeridos (DNI/NIE)
2. Identificarse a través de los mecanismos habilitados respectivos para DNI electrónico o certificado.
3. Con la finalidad de asegurar un nivel más elevado de seguridad, se deberá indicar un número de telefono al cual se enviará un PIN. Dicho PIN dará acceso al trámite electrónico.
4. Confirmación del número de teléfono introduciéndolo en la casilla habilitada.

[21] En caso de darse. Los teléfonos de atención al ciudadano funcionan bajo un sistema automático de atención que propone un conjunto de alternativas cerradas que pueden no encajar con la demanda del usuario. En dicho caso, la llamada se corta si proponer alternativas de servicio y/o atención personalizada

Una vez cumplimentados los pasos previos emergerá una ventanilla en la que se confirma que se ha dado de alta en el sistema cl@ve. Junto con la verificación se obtendrán los datos de registro (DNI/NIE, nombre y apellidos, número de teléfono, correo electrónico) y el código de activación para registrarse en cl@ve permanente.

4.3.1.2 Registro Básico

Con el registro básico, aunque no se concretan las limitaciones, se tendrán menores credenciales de acceso a los diferentes trámites de la administración. Este tipo de registro se puede realizar:

- A través de internet con carta de invitación

El registro básico a través de carta de invitación se divide en dos capítulos:

- Solicitud de la carta de invitación (por correo postal):
    - En primer lugar, el interesado deberá identificarse con su DNI o NIE tal y como se observa en el diagrama de flujos de la figura 9.
    - Una vez validados los datos, se optará por la opción de carta de invitación que saldrá en pantalla. En este momento, si la solicitud se ha guardado correctamente se procederá al envio de la carta al domicilio fiscal que conste en los datos de la Agencia Tributaria en ese preciso momento.

- Registro efectivo a través de carta de invitación:

Tras volverse a identificar con el documento pertinente el interesado deberá:

- Señalar que ya se dispone de la carta de invitación e ingresar los 16 caracteres del Código de Seguro de Verificación (CSV) ubicado en la carta de invitación
- Una vez validados los datos de identificación – DNI/NIE y CSV – habrá que aportar el teléfono móvil y el correo electrónico.

Una vez cumplimentados todos los campos y las respectivas validaciones se recibirá la confirmación de alta en el sistema de identificación. Del proceso en su

conjunto cabe tener en consideración el tiempo que se dilatará ya que más allá de los procesos que deban hacer online el envío de la carta ascenderá a 7 días laborales.

- A través de Internet por videollamada

El registro a través de videollamada, de igual modo que puede deducirse de las citas presenciales, dispone de un horario acotado[22] .

Tal y como vemos en el diagrama, para este tipo de registro se demandará un DNI, un correo electrónico y un teléfono, así como un ordenador con cámara, auriculares con micrófono y acceso a internet estable.

Tras identificarse con el documento identificativo pertinente se le dará paso al usuario, al cual se le recomienda realizar una llamada de prueba[23] asi como tener disponible el dispositivo con el cual se utilizará cl@ve.

En el momento de acceso se le da paso a una sala de espera virtual, una vez haya un operador accederá a la videoconferencia, haciéndose efectivo el registro si la identificación es fructífera.

Una vez efectuado el registro en el sistema clave por las diferentes modalidades habilitadas para tal fin, se dispondrá de un mecanismo de identificación electrónica que dará acceso a un número variable de trámites en función del tipo de registro – básico o avanzado - por el cual se haya obtenido.

4.3.2 Sistema de firma digital Cl@ve: Cl@ve firma

Dentro del sistema Cl@ve encontramos Cl@ve firma, aportando las funcionalidades de firma digital.

La obtención de cl@ve firma viene condicionada por:

- El acceso previo a un nivel de registro avanzado en el sistema Cl@ve permanente tal y como vemos en el diagrama de flujos 2 de la figura 9.

[22] El horario, tal y como se expone en el sitio web respectivo está disponible de lunes a jueves de 09:00 a 14:00 y de 15:00 a 18:00; viernes, de 9:00 a 14:00 (horario peninsular, y no disponible en festivos nacionales)

[23] Se recomienda a los interesados que realicen una prueba a fin de corroborar que efectivamente disponen de un dispositivo compatible con mecanismo de identificación, la videollamada.

- Tambien es necesaria la activación de Cl@ve permanente de acuerdo con su proceso de activación particular y en caso de ser pertinente – de acuerdo con el trámite de interés y el nivel de seguridad requerido – se proporcionará un nivel de garantía de autentificación más elevado mediante el sistema de verificación “One Time Password” (OTP)

Concluyendo, como hemos podido observar en el diagrama de flujos previo, el registro en el sistema cl@ve se trata de un proceso largo, fragmentado e interrumpido. En este sentido, el usuario no solo debe tener cierto nivel de habilidades digitales básicas, sino tambien cierto conocimiento técnico-conceptual del ecosistema de alternativas dentro del sistema cl@ve.

En el caso del sistema cl@ve, más allá de saber hacer uso de navegadores, asi como ir transitando por diferentes sitios web, no se requiere de conocimiento altamente tecnológico, sin embargo, sí que se torna esencial entender los diferentes mecanismos disponibles – cl@ve permanente, cl@ve PIN y cl@ve firma – así como los diferentes registros por los cuales los podemos obtener -registro básico y avanzado-. En este caso, saber que el registro básico no proporciona tanta seguridad y que, por ende, no tendremos acceso a tantos trámites es importante ya que tendremos que de escoger uno u otro tipo de registro en función de nuestras necesidades de acceso. Complementariamente, al existir cuatro modalidades de registro es necesario tener conocimiento de los requerimientos de cada uno para saber cuál se adecua más con los recursos a disposición o preferencias del interesado como llevar a cabo el proceso de manera semipresencial u online.

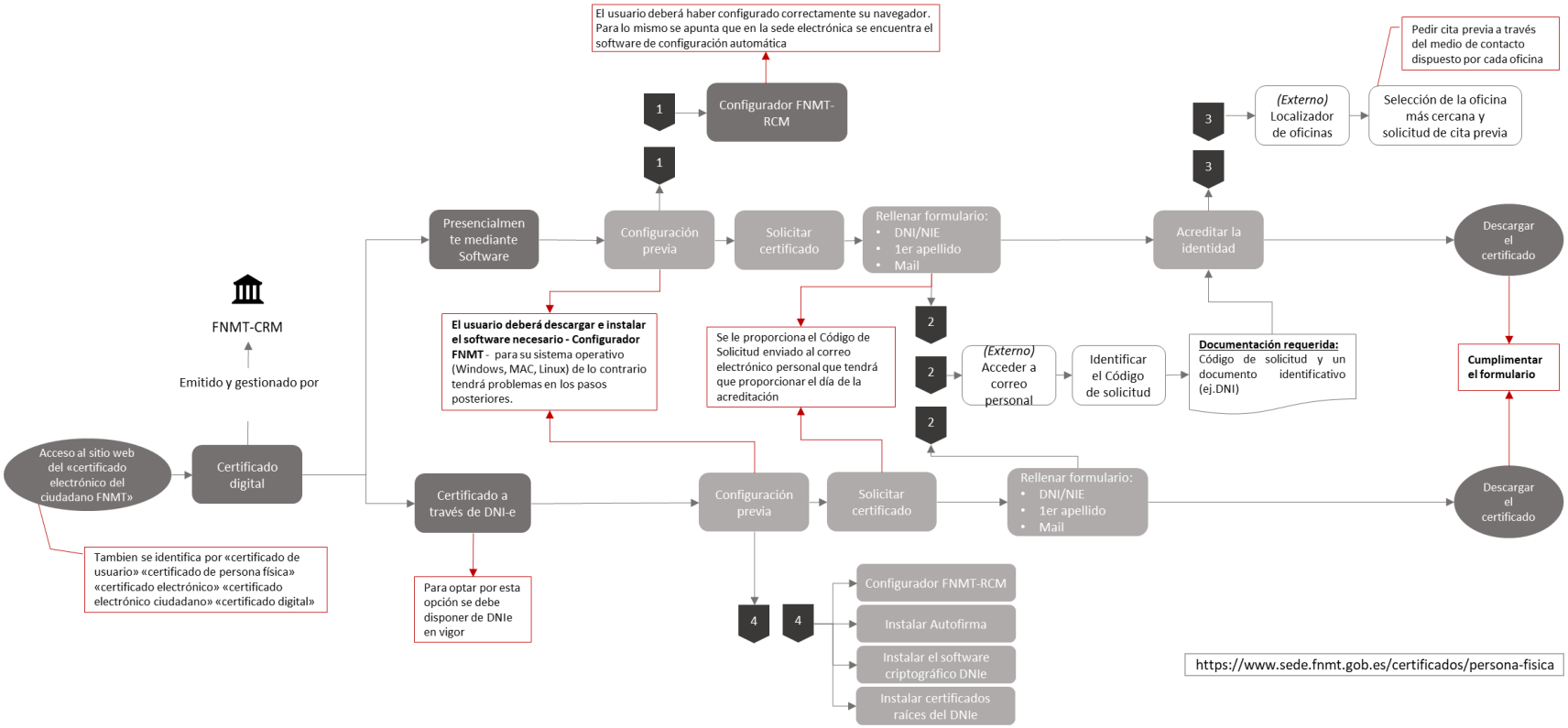
Por último, sería conveniente tener en consideración el coste de adquirir dichos mecanismos y es que adquirir cierto conocimiento sobre el ecosistema de mecanismos disponibles, sus funcionalidades asociadas, los diferentes medios para obtenerlos, asi como los propios tiempos del trámite supone un monto total elevado de horas dedicadas y movilización de recursos personales.

4.3.3 Certificado digital FNMT

Tal y como observaremos en la figura 10, el certificado digital gestionado y otorgado por la FNMT se puede obtener por dos vías:

Figura 10.

Diagrama de flujos del itinerario de registro para certificado digital FNMT-CRM



Fuente: Elaboración propia a través de sitio web «Certificado Digital» de la FNMT

4.3.3.1 Presencialmente mediante Software

El proceso de obtención del certificado digital presencial mediante software consta de 4 pasos de entre los cuales en uno el usuario deberá personarse en las Oficinas de Acreditación habilitadas.

1. De acuerdo con la FNMT, el primer paso implica la instalación del software necesario para la generación de claves «Configurador FNMT-RCM24»

En el enlace habilitado para acceder al sitio web con los diferentes enlaces al configurador, se contemplan las distintas versiones disponibles las cuales varían en función de:

   a. El sistema operativo del dispositivo en el que vaya a instalarse el software
   b. El tipo de unidad central de proceso (CPU):

- En el caso de los dispositivos Windows se contempla la opción de 32 y 64 bits. El conocimiento del número de bits del dispositivo en el que va a instalarse el software es imprescindible para que este se ejecute correctamente.
- En el caso MAC, a pesar de existir una única versión, en algunos casos será necesaria la habilitación de ciertos elementos para que el software se instale de manera satisfactoria. Complementariamente se apunta a que es imprescindible que el dispositivo cuente con chip M1 y tener instalada la aplicación «Rosetta»
- En el caso de Linux, se contemplan cuatro versiones, aquellas que hacen referencia al número de bits u otras especificaciones técnicas como si los dispositivos cuentan con RPM o DEB.

[24] Disponible en: https://www.sede.fnmt.gob.es/descargas/descarga-software/instalacion-software-generacion-de-claves
En el mismo enlace se contemplan los diferentes enlaces - de acuerdo con el sistema operativo y versión de dispositivo en el que vaya a instalarse el software – disponibles para efectuar la descarga del Configurados FNMT-RCM

Una vez cumplimentada la pre-configuración, antes de iniciar el proceso, el usuario ya tendrá que haberse enfrentado a un conjunto de requerimientos técnicos insalvables para alguien sin conocimientos tecnológicos.

2. El segundo paso contemplado en el proceso de obtención del certificado digital es la solicitud de este. Para lo mismo, debe cumplimentarse la «Solicitud de certificado FNMT de persona física» para los cuales se requiere cumplimentar un formulario con una serie de datos identificativos tal y como vemos en el diagrama de flujos de la figura 10.

Una vez cumplimentado el formulario se enviará la solicitud. Con el envio de la solicitud se le remitirá un correo electrónico con el código de solicitud, el cual deberá presentarse en la oficina de registro el día de la acreditación.

Para lo mismo, el interesado debe pedir hora en una de las Oficinas de Acreditación de Identidad habilitadas[25] para la acreditación de la identidad.

La FNMT habilita un buscador de oficinas[26] de carácter informativo sobre cuáles son las oficinas más cercanas y algunos datos de contacto. Asimismo, no es posible pedir cita previa de manera automatizada desde dicho localizador.

Dicha información de contacto no está homogeneizada ni establece contacto directo con la oficina en concreto. En algunas oficinas se identifica un telefono exclusivo para pedir cita previa el cual da acceso a un sistema de atención telefónica automatizada y de alternativas cerradas. El mismo informa de tramites generales no vinculados con la cita previa para una oficina de acreditación de la identidad.

En caso de no querer acceder a ninguno de los tramites mencionados por el sistema de atención automatizada o bien se informa al demandante de que no hay otra alternativa y se corta la llamada o bien se accede al servicio de cita previa.

En este se tiene que volver a informar del código postal – el mismo que el usuario había apuntado en el localizador de oficinas y por el cual se habían aportado el

[25] No todas las oficinas estan habilitadas para la identificación de todas las tipologías de interesados.
[26] Véase http://mapaoficinascert.aplicaciónspot.com/

contacto de la oficina a la que, en principio el usuario llama – y se le informará de la disponibilidad – en caso de haberla -. Puede darse que se informe al usuario de que no la hay y no se da alternativa, procediéndose a cortar la llamada o bien que efectivamente haya disponibilidad, una acotada a una alternativa que el usuario deberá aceptar tocando «1» en el teclado o bien contestando con un «sí» claro e identificable por el sistema de atención automatizado.

Asimismo, existen otras vías no documentadas en las páginas web oficiales como el correo electrónico a través del cual llevar a cabo el trámite de solicitud de cita previa para una oficina de acreditación de la identidad del demandante.

Debe tramitarse siguiendo los siguientes pasos:

1. Enviar un correo electrónico a la dirección «registro.«comunidad autónoma en la que vaya a realizar el trámite[27]»@correo.gob.es» manifestando qué se quiere tramitar.
2. Se le enviará un acuse de recibo. En este se informa del tiempo que se podria llegar a dilatar el trámite asi como alternativas de acceso a un trámite, entre otros.
3. Se le enviará una contestación al primer correo en el cual, entre otras cosas, se dispone lo siguiente «Para poder asignarle cita para la acreditación de la identidad en la obtención del certificado de persona física 2CA de la FNMT deberá responder a este correo indicando el nombre, apellidos y núm. de DNIe/TIE de la persona que precisa dicha acreditación, y revisen que todos los datos sean correctos, de lo contrario no se podrá adjudicar cita.» Complementariamente se informa de los documentos que el interesado deberá llevar a la cita presencial.
4. Contestar el mail con los datos requeridos.
5. El sistema le contestar con la disponibilidad existente a través de un listado de días y horas disponibles para acudir presencialmente a acreditar la identidad del interesado.

[27] Por ejemplo, en el caso de Cataluña el correo presentaría el siguiente formato «registro.catalunya@correo.gob.es»

En todo caso, esta alternativa no es publica, el usuario no tiene manera de saberlo más que mediante contacto telefónico y en caso de que el operador se la dé a conocer.

Una vez conseguida la cita previa para la acreditación de la identidad por medios físicos, el ciudadano podrá acudir el día concertando, aportando un documento identificativo, así como el código de solicitud.

Por último, una vez descargado el configurador, solicitada la petición, acreditada la identidad mediante cita previa en una cita presencial, se podrá descargar el certificado pertinente[28]. Si bien antes, deberán cumplimentarse una serie de datos en posesión del interesado:

- Nº del documento de identificación
- Primer apellido del interesado
- Código de solicitud recibido

Complementariamente a la vía presencial a través de software, se contempla otra vía, a través de DNI-e, la cual se expondrá a continuación:

4.3.3.2 Certificado a través de DNI-e

Esta alternativa se trata de una íntegramente en remoto dado que, al realizarse a través de DNIe la acreditación de la identidad del usuario ya se efectuó.

De este modo, se podria obtener el Certificado de Persona Física sin necesidad de volver a acreditar la identidad en una Oficina de Registro.

El proceso presenta alta similitud con el proceso a seguir en el caso de Certificado Software y tal y como observamos en el diagrama de flujos de la figura 10.

En este caso, vemos como la preconfiguración requiere de la instalación de mayor número de elementos, tres de los cuales se encuentran en sitios web externos, en este caso en el Portal de Administración electrónica y en el sitio web de la Policía Nacional. Complementariamente, para todos los elementos cabe

[28] Este debe descargarse en el mismo ordenador en el que se descargó del Configurados FNMT-RCM e introducir los mismos datos que se aportaron en la solicitud.

tener en consideración el sistema operativo y el tipo de unidad central de proceso (CPU)

3. Solicitar el certificado digital con un certificado válido – DNIe en este caso - con el que identificarse para solicitar el certificado de persona física. De igual modo que en la anterior alternativa, se enviará al correo del interesado un correo con el Código de Solicitud para poderse descargar el certificado.
4. Descargar el certificado mediante el Código de Solicitud a través del sitio web habilitado.

Como se acaba de exponer observamos que, en el caso del certificado electrónico, se nos dan dos alternativas a través de las cuales obtener dicho mecanismo, si bien no, en este caso la elección de uno u otro modo no determinará el nivel de credenciales que obtendremos y por ende el número de tramites a los que tendremos acceso[29]. No obstante, sí que tendremos que indagar en la modalidad que se adecue mejor a nuestras preferencias. En caso de tramitarlo a través de la opción identificada como «Certificado Software» deberemos acudir presencialmente a una de las oficinas habilitadas para acreditar nuestra identidad. En este caso, esta es la única en caso de no tener operativo el DNIe, medio que se propone como alternativa.[30]

Por último, vemos como, del mismo modo que en el caso del sistema cl@ve, a la hora pedir cita para acreditar la identidad, el usuario tendrá que contactar directamente a cada una de las oficinas disponible, teniendo en cuenta que las oficinas podrán disponer de teléfono móvil, correo electrónico o sitio web habilitado a través del cual solicitar la cita. Cabe resaltar la heterogeneidad de los medios de contacto, así como de los procedimientos a seguir.

Cabe tambien tener en consideración los tiempos de espera para cada una de las oficinas asi como la ubicación de la oficina asignada.

[29] El certificado electrónico, independientemente de a través del medio por el cual lo obtengamos nos otorga un nivel de seguridad total, dándonos acceso a todos los tramites que queramos llevar a cabo

[30] En este caso, el certificado electrónico no aportaría mayores credenciales que las que ya aporta el DNIe

4.3.4 DNI electrónico

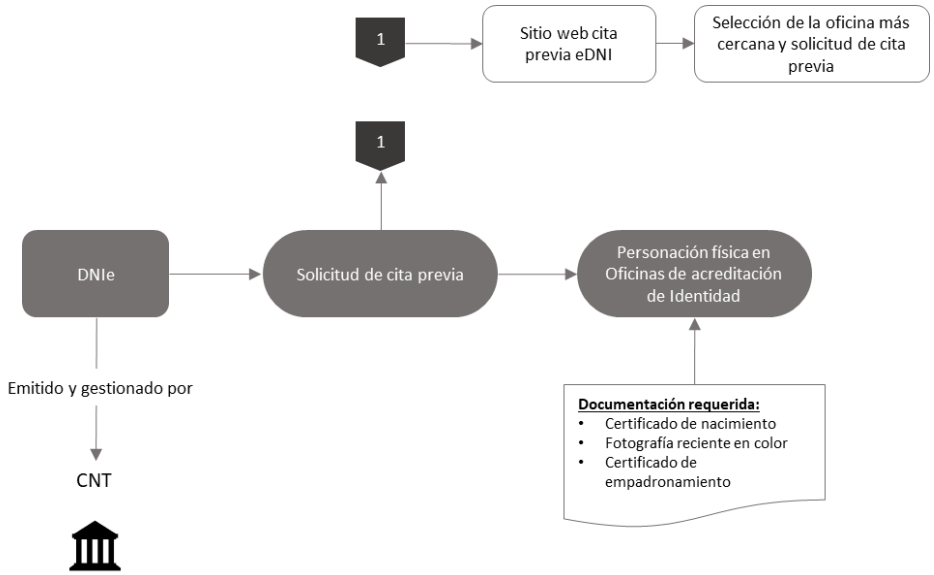
La versión DNI 3.1 emitida desde 2015, alberga en su chip una serie de claves digitales, las cuales son sustento de los certificados que integra. Esto es, la obtención del DNI electrónico esta inherentemente vinculado con la obtención del DNI físico.

Consecuentemente, para la obtención del DNI y los certificados albergados en el mismo se deberá acudir a una Oficina de Expedición del DNI, abonar la tasa pertinente y presentar los documentos que se requieran tal y como observamos en el diagrama de flujo 4.

En el momento de expedición del DNI se proveerá al demandante con un PIN, indispensable para el uso del DNI electrónico. Este puede ser modificado en los Puntos de actualización del DNI electrónico (en adelante PAD) disponibles en las Oficinas de Expedición. En caso de no recordar el PIN o que esté bloqueado – y quiera modificarse – el interesado podrá identificarse con la huella dactilar.

Figura 11.

Diagrama de flujos del itinerario de registro para DNIe



Fuente: Elaboración propia a través del sitio web del «DNIe» del Cuerpo Nacional de Policía

En este caso, el diagrama de flujos nos describe un proceso íntimamente relacionado con la obtención del DNIe, dado que, no podemos poseer el DNIe sin su soporte físico, el DNI tradicional.

En este caso, el sitio web solicitud de cita previa si posee un buscador de oficinas integrado en el que es posible seleccionar la oficina a la que acudir junto con el día y la hora deseada[31]

4.4 Uso de los mecanismos de identificación electrónica

En el siguiente capítulo y como última línea de investigación, se procederá a exponer los aspectos técnicos *sine qua non* no se puede hacer uso efectivo de los diferentes mecanismos de interacción con la Administración Pública por medios electrónicos.

Complementariamente, más allá de la descripción detallada de todos los pasos a seguir, los requerimientos técnicos, los elementos software y hardware necesarios, se destacarán incongruencias u otro tipo de errores a lo largo del proceso de «puesta en marcha» de los diferentes mecanismos.

4.4.1 Uso de sistema Cl@ve

4.4.1.1 Cl@ve permanente

El mecanismo de cl@ve permanente, dada la naturaleza y características de su sistema, deberá sin excepción, ser activada antes de su primer uso y tras el registro en el sistema cl@ve. Para lo mismo, el usuario deberá acudir al apartado «Características de la contraseña» en el apartado de cl@ve permanente y en concreto en el enlace del servicio de activación y rellenar el formulario con los datos requeridos tal y como se apunta en el diagrama de flujos de la figura 9.

En caso de que los datos sean correctos, se enviará un OTP mediante SMS al móvil del demandante. Dicho PIN deberá introducirse en la casilla habilitada en el PC a través del cual se esté tramitando.

[31] Véase: https://www.citapreviadnie.es/citaPreviaDni/

Una vez confirmados los datos, se le permitirá al interesado crear la contraseña de la cl@ve.

Una vez activada la cl@ve, para su uso de cara a utilizarlo para acceder a un trámite, serán necesarios los siguientes pasos, de igual modo, estipulados en el propio sitio web de Cl@ve permanente:

- Una vez se haya accedido al trámite deseado, se deberá seleccionar la opción de acceso de cl@ve permanente. Una vez seleccionada se deberá introducir tanto el DNI como la contraseña establecida previamente.
- En caso de que el trámite al que se quiera acceder requerirse un nivel de seguridad superior, se haría uso del OTP. Este se enviaría mediante SMS al dispositivo móvil del ciudadano.

La demanda de doble verificación mediante un OTP podrá estar condicionada por el tipo de registro a través del cual se obtuvo la cl@ve. Asimismo, el ciudadano no puede predecir las situaciones en las que esta doble verificación se solicitará.

Aspectos destacables del proceso de activación de la cl@ve permanente son que las referencias a la activación de la cl@ve son vagas, se mencionan como un punto más entre toda la información que se recibe al registrarse y no se hace referencia o se habilita un enlace a partir del cual llevar a cabo el proceso.

En este caso, tendría que ser el usuario el cual, por medios propios descubriese que este se encuentra en el apartado de cl@ve permanente > características de la contraseña[32], lugar en el cual encontramos el acceso al servicio de activación. Para el mismo servicio el usuario, deberá tener a mano el dispositivo movil a partir del cual recibir el OTP indispensable para activar el mecanismo.

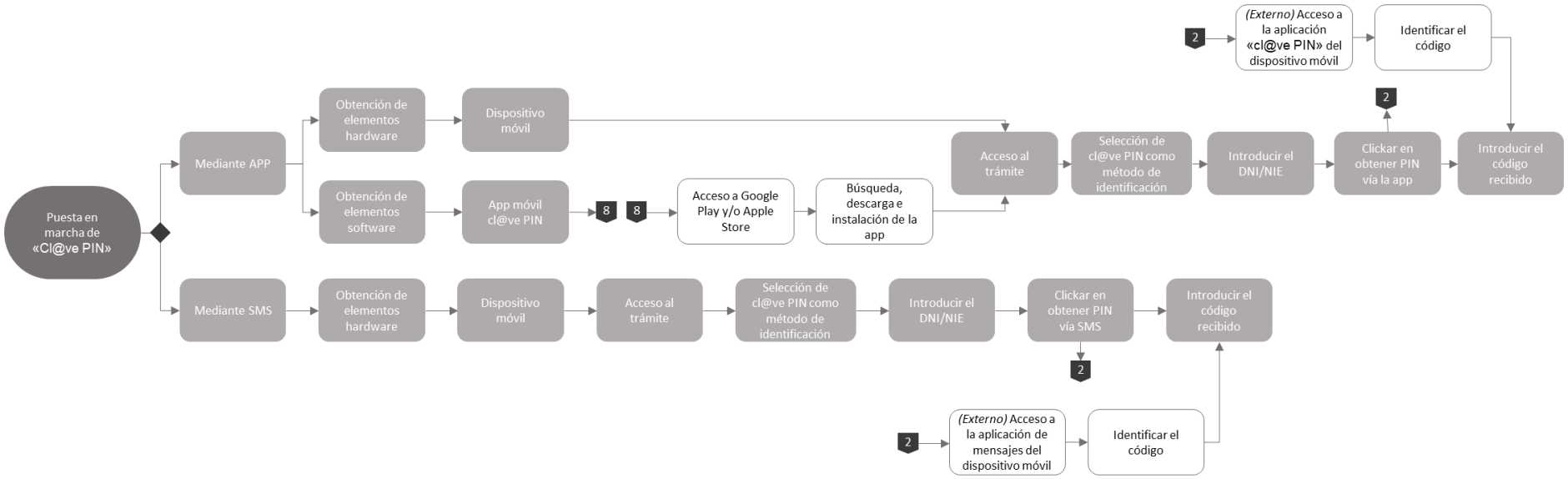
4.4.1.2 Clave PIN

Clave PIN trata de un sistema de acceso electrónico de un solo uso al cual se puede tener acceso mediante dos vías que a continuación se detallan gráficamente.

[32] Véase: https://clave.gob.es/clave_Home/Clave-Permanente/Procedimientos.html

Figura 12.

Diagrama de flujos del uso del mecanismo cl@ve PIN



Fuente: Exposición gráfica del itinerario de uso de cl@ve PIN. Elaboración propia a partir del sitio web de «cl@ve»

- Mediante aplicación móvil (Cl@ve PIN): Opción que implica la realización de un conjunto de pasos que van desde: la descarga de la aplicación de «Cl@ve PIN» – disponible tanto para dispositivos Apple como Android – pasando por la activación de la aplicación[33] en la cual recibirás las claves PIN en el momento de querer acceder a un trámite electrónico.
  Para recibir dichos códigos tal y como se muestra en el diagrama de flujos de la figura 12, una vez el interesado se encuentre en el trámite deseado deberá introducir su DNI/NIE asi como la fecha de validez del DNI (o fecha de expedición si es un DNI permanente)
  El PIN proporcionado se habra enviado al dispositivo activado y permanecerá visible durante un tiempo limitado (10').

- Mediante SMS: De igual modo que mediante aplicación móvil, en el caso de que optemos por la opción de SMS, una vez en el sitio web del trámite deseado, se deberá introducir el DNI/NIE, así como la fecha de validez del DNI (o fecha de expedición si es un DNI permanente). Tras introducir los datos demandados se pulsará la opción de «Obtener PIN» y solicitar el envío de SMS. Con el PIN que se habrá enviado a el dispositivo móvil del interesado se deberá validar la cl@ve PIN en un tiempo inferior a diez minutos.

4.4.1.3 Clave firma

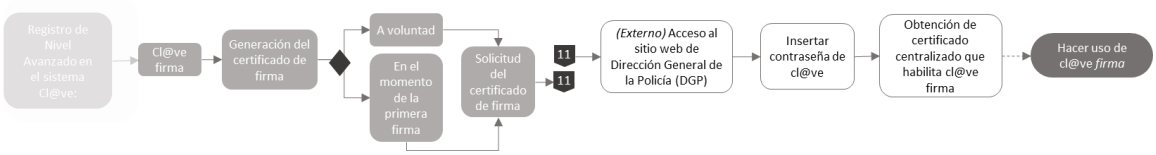
Cl@ve firma permite la firma digital de documentos electrónicos mediante certificados electrónicos centralizados.

Para el uso efectivo de dichos certificados el interesado tendrá que solicitarlos siguiendo el siguiente procedimiento:

[33] Para la activación de la aplicación será necesario introducir el DNI/NIE del interesado, así como la fecha de validez del DNI (o fecha de expedición di es un DNI permanente) e introducir el código de activación que se le enviará mediante SMS al dispositivo móvil con el que se registró en el sistema Cl@ve. Una vez cumplimentados los tres campos Cl@ve PIN quedará activado en el dispositivo utilizado.

Figura 13.

Diagrama de flujos sobre la generación de certificado de cl@ve firma



Fuente: Elaboración propia a partir del sitio web de «cl@ve»

- A voluntad del interesado, tal y como se expone en el sitio web, en el apartado de «realización de la firma» el interesado puede generar las claves de autentificación y firma a voluntad e independientemente de la realización de un trámite en concreto.
- En caso de no haber solicitado previamente los certificados de firma, en el momento de realizar un trámite, el sistema dará la opción de demandarlo. Por lo mismo, el interesado se verá redirigido a un sitio web bajo custodia del Cuerpo Nacional de Política.

En caso de haber solicitado correctamente los certificados, el interesado será redirigido a el sitio web del trámite que pretendía llevar a cabo el trámite inicial.

Como se observa en el diagrama de flujos de la figura 13, en ambos casos, el usuario se verá redirigido a un sitio web externo, el del Cuerpo Nacional de Policía, puesto que es el cuerpo encargado de la custodia de los certificados centralizados.

Llegado el momento en el que interesado esté en posesión de los certificados pertinentes podrá proceder a la firma de los documentos que se le requieran.

A la obtención de los certificados se le complementan los requisitos previamente expuestos en el apartado de « 4.3.1. Sistema de identificación Cl@ve: Cl@ve permanente, Clave PIN », lo veíamos en el diagrama de flujos de la figura 9, en el cual vemos como para realizar la solicitud de cl@ve firma, el usuario debe haberse registrado mediante una modalidad de «Registro Avanzado» y haber activado su cl@ve permanente, es por ende, dependiente de estos previos.

4.4.2 Uso de Certificado digital

Una vez se ha efectuado adecuadamente el registro mediante la personación en las Oficinas de Acreditación, el interesado, como se ha comentado previamente, deberá descargar los certificados en el equipo con el que se realizó la solicitud, así como en el equipo en el que se utilizará.

Para la descarga del certificado será necesario estar en posesión del NIF o NIE, el primer apellido y el código que se le envia en el momento de verificar la identidad. Una vez introducido, la aplicación se procederá a abrir en el equipo y se tendrá que introducir la contraseña que se introdujo en el momento de hacer la solicitud.

Tras lo previo, el sistema procederá a la instalación del certificado digital demandando en los almacenes de certificados del sistema operativo del equipo utilizado. Posibilitando el uso de los certificados en cualquier navegador del equipo.

4.4.3 Uso de DNI electrónico

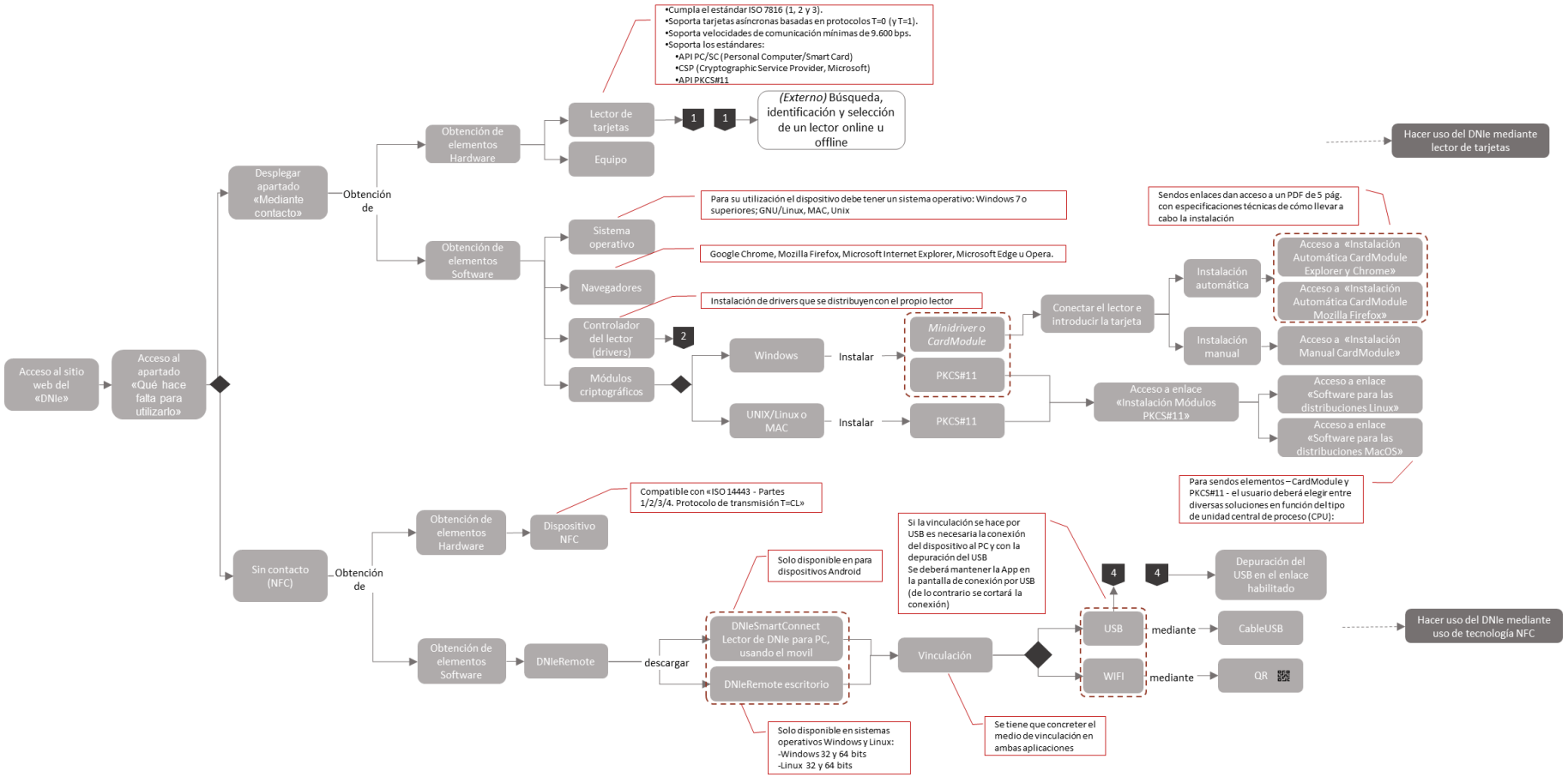
Para el uso efectivo del DNIe se tiene que contar con una serie de requisitos de software y hardware previos que permitan el acceso al chip contenedor de los certificados de identificación y firma.

Para los nuevos DNI 3.0[34], tal y como vemos en el diagrama de flujos expuesto a continuación, es posible conectarse a la tarjeta mediante dos modos

[34] Solo a través de DNI posteriores al 2015

Figura 14.

Diagrama de flujos del itinerario de puesta en marcha para DNIe



Fuente: Elaboración propia a partir de sitio web del «DNIe»

4.4.3.1 Mediante lector de tarjetas (contacto)

Sin duda, el mecanismo de identidad digital que requiere de mayor conocimiento técnico es el DNIe. Tal y como hemos podido observar en el diagrama de flujos de la figura 14, se requiere de la adquisición, adecuación e instalación de múltiples elementos que en conjunción habilitan el uso del DNIe. En el caso del DNIe mediante el uso de un lector de tarjetas se demanda al usuario de un lector que cumpla con un listado de especificaciones técnicas – especificaciones con las que un público medio puede no estar familiarizado -:

Asimismo, más allá de las especificaciones técnicas respecto a los requisitos con los que debe cumplir el lector, no se ha habilitado un lugar de referencia para la adquisición y/o un lector en concreto. Sino que, en este caso, es el usuario por los canales que considere pertinentes que tendrá que buscar y comprar un lector de tarjetas.

Respecto a los elementos software para el ordenador, deben cumplirse con cuatro aspectos básicos:

- Se deberá tener en consideración el sistema operativo y hacer las adecuaciones pertinentes en caso de ser pertinente.
- A pesar de manifestarse la compatibilidad con todos los navegadores, se reportan mejores experiencias con Google Chrome (93%) o Mozilla Firefox (86%)[35]. Asimismo, tambien funciona con otros como Microsoft Internet Explorer, Microsoft Edge, Chrome u Opera.
- Complementariamente al lector de tarjetas, el usuario tendrá que buscar, descargar e instalar los drivers necesarios para el uso del lector. Estos drivers tal y como se apunta en el sitio web del DNIe - «Para operar con un lector de tarjetas inteligentes, será necesario instalar un driver que, normalmente, se distribuye con el propio lector» - debe ser el usuario quien los busque.
- Por último, tal y como se expone en el Manual del DNIe el equipo debe tener instaladas unos módulos criptográficos necesarios para una interacción adecuada con las tarjetas criptográficas, en este caso con el

[35] Véase: ¿Son claros los trámites digitales? Prodigioso Volcán pg.78

DNIe. Como se observa en el diagrama de flujos se deberán instalar diferentes módulos criptográficos en función del sistema operativo, el tipo de unidad central de proceso (CPU) e incluso en función del navegador en el que se instalará.

En este sentido, el sitio web no ayuda puesto que no da acceso exclusivo al software que se requiere descargar, sino que da acceso a fuentes con información complementaria a esta, siendo complejo distinguir a que enlace hace falta acceder para descargar el software de interés.

4.4.3.2 Mediante antena sin contactos (NFC)

Tras la implantación del DNI3.0 en 2015, todos los soportes expedidos tras dicha fecha tienen habilitado su uso sin contacto a través de la tecnología NFC.

De acuerdo con el sitio web oficial del Cuerpo Nacional de Policía en el apartado «Cómo utilizar el DNI» → «Que hace falta para utilizarlo[36]» son necesarios elementos hardware y elementos software:

- Hardware: Se debe contar con elementos hardware, en este caso con un dispositivo con la tecnología NFC con las especificaciones técnicas que apunta en la figura 14.
- Software: De igual modo, tambien se debe disponer de algunos elementos software.
    - Según el presente sitio web será necesario descargar una «APLICACIÓN que utilice el DNI 3.0 para identificar al usuario y acceder a un servicio específico o para firmar electrónicamente un documento con igualdad jurídica que la firma manuscrita». Complementariamente se dispone que «Para su instalación, proceda a descargar la APLICACIÓN desde un repositorio oficial (Google Play/Apple Store...)»
    - Complementariamente, se apunta a la necesidad de un lector que sea compatible con el DNI3.0 que cumpla con las especificaciones técnicas dispuestas en la figura 14.

[36] Disponible en: https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_300&id_menu=15

Contrariamente, en la «GUIA DE REFENCIA DEL DNIE CON NFC» en el apartado de «requerimientos software», no se hace referencia a la necesidad de ningun tipo de lector de tarjetas y tampoco se contempla la opción de descargar la aplicación en Apple store «Para su instalación habrá que acceder al repositorio de APLICACIÓN (Google Play….) y proceder a su descarga e instalación»

Profundizando en el analisis, complementariamente a las fuentes consultadas previamente – sitio web del DNIe y la Guía de referencia del DNIe con NFC - en el «Área de descargas[37]», encontramos información más detallada respecto a los requerimientos necesarios para el uso efectivo de la tecnología NFC y en concreto, se detalla la información relativa a la famosa aplicación – de la cual hemos hablado previamente - necesaria para el uso de DNIe mediante NFC.

Se hace referencia al nombre de esta como «DNIeRemote» y se dispone que esta “aprovecha la tecnología NFC para convertir el dispositivo móvil en un lector del DNIe 3.0 conectado al PC, permitiendo así acceder a los servicios de la administración electrónica que requieren de autenticación con certificado digital, y realizar firmas digitales en documentos a través de las correspondientes aplicaciones” (Cuerpo Nacional de Policía, 2023)

Seguidamente se apunta a que esta aplicación funciona en conjunto a la aplicación para Android "Lector de DNIe para PC, usando el movil". De esto, el usuario puede deducir por primera vez que, la aplicación no se encuentra disponible para sistema operativo de Apple y que la aplicación móvil funciona en conjunción con otra aplicación, en este caso de escritorio.

A continuación, se disponen una serie de enlaces para la descarga de DNIeRemote escritorio - cuando en ningun lugar previo se había indicado directamente de la existencia de esta -.

Mas tarde si, en el «Manual completo de la aplicación sobre el funcionamiento y las opciones de configuración» se apunta a que ambas aplicaciones funcionan en “tándem”. En este se concreta que la aplicación DNIeRemote se compone de dos módulos:

[37] Disponible en: https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_1015&id_menu=65

- La aplicación para escritorio para los sistemas operativos Windows/Linux
- Una aplicación Android para el dispositivo móvil

Para la descarga de DNIeRemote en escritorio se deberán tener en consideración algunos aspectos técnicos de compatibilidad en función del dispositivo en el que se vaya a ejecutar la aplicación, asi como el tipo de unidad central de proceso (CPU).

En el caso de la aplicación del dispositivo móvil, vemos que en este caso se hace referencia a ella como DNIeSmartConnect, así dice textualmente, “Esta Aplicación para sistemas operativos Android se obtiene a través de Google Play. Se localiza con el nombre DNIeSmartConnect vinculada al desarrollador CNP-FNMT. Contrariamente, en el sitio web del «Área de descargas» veíamos como se hacía referencia explícita al nombre de la aplicación como "Lector de DNIe para PC, usando el movil".

Más allá de las aplicaciones a descargar, existen alternativas por lo que respecta a la conectividad entre el dispositivo movil y la aplicación de escritorio, y es que esta se puede llevar a cabo a través de USB (sólo en Windows[38]) o a través de WIFI (asegurándonos que ambos dispositivos estan conectado a la misma red).[39]

En el presente manual – el Manual completo de la aplicación sobre el funcionamiento y las opciones de configuración – tambien se detallan los pasos a seguir para poder hacer un uso efectivo de la tecnología propuesta.

Para el uso, lo primero que se apunta en el manual, es que, es necesario la carga y vinculación del DNIe con los sistemas operativos Windows/Linux, a través de la aplicación de escritorio de DNIeRemote y la aplicación para dispositivos móvil.

Para lo mismo se dispone la necesidad de seguir los siguientes pasos:

- Ejecución de la aplicación de escritorio: tal y como se expone en el mismo manual, para acceder a los certificados digitales del DNIe 3.0 en el ordenador, es necesario completar la conexión entre este y el dispositivo móvil a través de la aplicación de conexión DNIeRemote. Para ello, se

[38] En el documento de análisis, punto 3.2, se hace referencia a y cito literalmente “Windowos”
[39] El modo de conexión se tendrá que concretar explícitamente tanto en la aplicación para el dispositivo móvil como en la aplicación de escritorio.

tendrá que ejecutar la aplicación en el ordenador, previamente descargada a través de los enlaces habilitados en el «Área de Descarga»

- Puesta a punto de la aplicación móvil: los pasos a seguir para la puesta en marcha de la aplicación son:
    - Selección del sistema operativo del PC
    - Selección del medio de conexión (Wifi o USB)
    - Efectuar la vinculación capturando el QR o conectándolo directamente a través del cable USB.

Una vez efectuada la vinculación entre ambos dispositivos se deberá presentar el DNIe 3.0 en el dispositivo móvil para iniciar la comunicación a través de NFC.

Complementariamente a los elementos hardware y software detallados previamente, para la tramitación de determinado servicio y/o acción perceptible de utilizar las certificaciones del DNIe, se deberá tener acceso al PIN que se proporcionó en el momento de obtener el DNIe.

En caso de no recordarlos o querer modificarlos, el interesado debe acudir presencialmente a los Puntos de Actualización del DNI electrónico (PAD) ubicados en las oficinas de expedición de los DNI y sin necesidad de pedir cita previa.

Por último, en el presente capítulo, se hará referencia a otros aspectos vinculados al uso de los mecanismos descritos, y que, perceptiblemente, podrían complejizar su uso.

Tal y como se observa en el último diagrama de flujos expuesto, la puesta en marcha del DNIe tanto mediante contacto como sin contacto con la tecnología NFC requieren de la adecuación de cuantiosos elementos altamente técnicos, tanto hardware como software.

Sin ir más lejos vemos como con tal de hacer uso del DNIe mediante contacto tendríamos que disponer de un lector de tarjetas específico, un sistema operativo actualizado, asi como controladores del lector y módulos criptográficos adaptados al sistema operativo del equipo en el que se instalan. Un total de cuatro requisitos técnicos indispensables para hacer uso del DNIe mediante

contacto. Del mismo modo que mediante contacto, con la alternativa *contactless* tambien se le requieren al usuario una serie de especificaciones técnicas asi como, la búsqueda descarga e instalación de dos aplicaciones que trabajan en tándem, o la vinculación de ambas.

Asimismo, más allá de los requerimientos altamente técnicos, lo más complejo es encontrar y entender la información al respecto de dichos requerimientos. Tal y como se ha observado a través del análisis, la información se encuentra fragmentada en fuentes de diferentes niveles de detalle, en sitios y/o apartados webs no intuitivos, en los que se dispone información incorrecta o no se encuentra, etcétera.

4.5 Barreras a la identidad digital

De acuerdo con el analisis realizado, se proceden a exponer los elementos complejos identificados en el analisis que podrían erigirse como barreras a la aceptación y uso de la identidad digital y ser partícipes del desajuste entre oferta y demanda de servicios públicos digitales.

De acuerdo con lo interpuesto en la LPACAP, en su artículo 14, los ciudadanos tienen el derecho y la obligación a relacionarse a través de medios electrónicos con la Administración Pública en aquellos casos en los que se establezca la obligación.

De acuerdo con lo previo, la Administración Pública debería garantizar la existencia de mecanismos de interacción efectivos, de uso intuitivo y conveniente para al ciudadano.

Si se tiene como objetivo lo previo - unos mecanismos usables, intuitivos y accesibles para el conjunto de la ciudadanía - tendrían que solucionarse o disiparse algunas de las barreras identificadas en el analisis.

Las barreras identificadas las categorizaremos según su naturaleza:

- Elementos complejos en sí, dada su naturaleza altamente técnica o que requiere de un conocimiento previo como son los elementos de carácter

tecnológico o los conceptos y terminología utilizada en todo lo que envuelve la identidad digital.

- Elementos que por naturaleza no son complejos pero que dado el formato en el que se encuentran actualmente, pueden complejizar la comprensión y la puesta en marcha de los diferentes mecanismos de identidad digital.

Por lo que respecta a los elementos considerados complejos en si por su alto carácter técnico encontramos 2 grandes barreras.

4.5.1 Barrera 1: Frontera antinatural y difusa entre los actos de identificación electrónica y los actos de firma digital en un ecosistema de múltiples identidades.

La idea de «identidad digital» y su manifestación a través de los actos separados entre la identificación electrónica y la firma digital puede resultar compleja de comprender.

Tal y como identificábamos en el primer apartado «4.1 Ecosistema conceptual de la identidad digital», conceptos tan interiorizados y naturalizados como la «identidad tradicional» la cual, se manifiesta mediante la auto evidencia del yo para identificarse y la firma manuscrita, para expresar voluntad y consentimiento, contrasta con la realidad del «identidad digital»

En esta, como se venía diciendo, no solo existen mecanismos distintos para los actos de identificación electrónica y firma digital, sino que existen diversos mecanismos para cada uno de dichos actos.

Los principales elementos por los cuales se sustenta dicha diferenciación[40] regulada por Ley[41] son los principios de «proporcionalidad» y «minimización de datos». Por lo mismo, se dispone que se tendrá que hacer uso de unos determinados mecanismos para la identificación electrónica y uso de otros para la firma digital.

[40] Dicha diferenciación, vemos que, no se da en el caso del canal físico, es decir, un ciudadano no tiene que valerse de diferentes mecanismos para identificarse y expresar voluntad y consentimiento. Como vemos la identidad digital introduce nuevos procederes y conceptos no controlados por la ciudadanía.
[41] PACAP

No obstante, a dicha distinción funcional[42] se le introducen algunos elementos que podrían difuminar dicha distinción y complejizar el entendimiento de las funcionalidades y límites de cada uno. Estos son los articulos 10.3 y 10.4 de la LPACAP en los que, respectivamente, se expone que cuando asi lo disponga la normativa reguladora aplicable las Administraciones Públicas podrán admitir los mecanismos de identificación – contemplado en el apartado 2 del mismo precepto – como sistema de firma y cuando el interesado haga uso de los sistemas de firma digital – regulados por la Ley – su identidad se entenderá acreditada.

Vemos como, la línea que separa uno del otro es algo difusa. Esto, según Bernal (2022, pg. 306) tiene sentido por razones de económica, es decir, ¿Por qué un usuario haría uso de otro medio de identificación si con los mecanismos de firma ya se le permite al firmante acreditar su identidad? Dicha flexibilidad podría difuminar la diferencia entre sistemas de identificación electrónica y firma digital introducida a través de la LPACAP con el fin de simplificar la intervención de los interesados en el procedimiento administrativo (Bernal, 2022, pg.306). Complementariamente, podría llegar a generar confusión e incerteza jurídica dada la incapacidad para determinar con antelación cual será el mecanismo necesario para interaccionar con la Administración Pública.

A la difusa distinción entre los actos de identificación electrónica y firma digital debemos sumarle la multiplicidad de mecanismos de identificación electrónica y firma digital existentes. En el caso español, el ecosistema de identidades digitales está compuesto por diversos mecanismos entre los que encontramos las soluciones de la figura 7 «Soluciones de identidad digital en España», arriba expuesta.

Esto no solo podría resultar incomprensible de entrada, sino que complementariamente supone mayor esfuerzo y recursos a fin de determinar aspectos como ¿Qué aspectos les diferencian? ¿Qué funcionalidades tienen asociadas? ¿Qué nivel de seguridad[43] aporta cada uno de ellos? ¿Cuáles son

[42] De acuerdo con la PACAP (art. 11) para cualquier actuación prevista con la Administración Pública, será suficiente con el uso los mecanismos de identificación electrónica y solo en algunos casos será obligatorio el uso de los mecanismos de firma digital[42].

[43] Complementariamente, se le añade la complejidad para determinar el tipo de mecanismo a utilizar en función de la seguridad requerida para la interacción con la Administración. Es decir,

los requisitos para el registro? ¿Quién es la entidad que los emite y gestiona? ¿Cuáles son los diferentes métodos de registro? ¿Qué elementos necesito para cada uno de los métodos de registro? ¿Qué elementos (software y hardware) son necesarios para la puesta en marcha de cada uno de los mecanismos?

Por lo que respecta a la distinción por nivel de seguridad aportado, vemos como se producen incoherencias en las credenciales que aporta cada mecanismo y por ende una distinción difusa entre ellos por nivel de seguridad aportado. Como hemos observado, puede darse que en determinado trámite se acepte un mecanismo que aporte seguridad tipo 3 y no otro que aporte el mismo nivel de seguridad.

La existencia de múltiples mecanismos de identidad digital y la línea difusa que las distingue, a veces imperceptible, junto con las incoherencias y la discreción de la Administración Pública para requerir uno u otro implica estar siempre bajo la duda de que mecanismo será necesario o cual será suficiente.

4.5.2 Barrera 2: Componentes altamente tecnológico

El componente altamente técnico es frecuente a lo largo de todos los procesos analizados tal y como hemos podido observar en los capítulos analítico-descriptivos de los mecanismos de identidad digital.

Dicho carácter técnico se agudiza en el plano de lo tecnologico, y es que, como puede deducirse, se tendrá que hacer uso de medios electrónicos a lo largo de todo el proceso. Dicha complejidad tecnológica está especialmente vinculada con la obtención y uso de elementos software y hardware requeridos para la puesta en marcha de los diferentes mecanismos de identificación electrónica y firma digital.

Tal y como hemos podido observar en los capítulos de análisis de los diferentes mecanismos el que requiere de mayor número de elementos hardware y

dada la existencia de cuatro niveles de seguridad requeridos - 0,1,2 y 3 – y los diferentes niveles aportados por los diferentes mecanismos, resulta dificulta saber cuál será el mecanismo indicado para cada trámite. Complementariamente, el usuario no sabe qué nivel de seguridad se le va a requerir hasta que esté realizando el trámite y se le notifique que el mecanismo que está utilizando no aporta la suficiente seguridad para llevar a cabo el trámite en curso.

software es el DNIe. A continuación, se identifican algunos casos en los que dicha complejidad queda evidenciada.

- **DNIe con lector de tarjetas (contacto)**

Hacer uso del DNIe mediante contacto requiere de la adquisición de un elemento hardware imprescindible, el lector de tarjetas. Este, tal y como hemos podido observar en el diagrama de flujos de la figura 14 se tiene que contar con un seguido de especificaciones técnicas sin las cuales no podriamos hacer uso de nuestro DNIe para los fines predispuestos. En este caso, es el usuario, que sin mayor guía que las especificaciones en lenguaje técnico tendrá que buscar por los medios que vea convenientes, el lector que vaya a utilizar.

La búsqueda de un dispositivo de dichas características para un ciudadano sin conocimientos tecnológicos elevados puede suponer una barrera de entrada al uso del DNIe.

Asimismo, una vez se disponga de dicho dispositivo – el cual se obtiene en el libre mercado y en caso de haber dado con un que se adeque a las especificaciones técnicas – el proceso de instalación en el equipo en el que se vaya a hacer uso, tambien puede suponer problemas para el usuario. El uso efectivo de dichos dispositivos implica la instalación de unos *drivers* lo cual tambien puede suponer problemas al no existir una guía oficial para su efectiva instalación, sino que, como se comentaba previamente, es el fabricante del lector el cual perceptiblemente aportará las instrucciones de instalación.

Complementariamente a los elementos hardware se necesitará de la instalación de elementos software en el equipo en el que se vaya a hacer uso. En este caso serás unos módulos criptográficos que tambien deben instalarse y ejecutarse en adecuación al sistema operativo y el tipo de unidad central de proceso (CPU) del equipo.

- **DNIe mediante antena sin contacto (NFC):** en la misma línea que en el caso del DNIe mediante contacto, el uso del DNIe mediante la tecnologia NFC requiere la búsqueda, descarga y adecuación de múltiples elementos, en este caso mayoritariamente de software.

Disponer de un dispositivo NFC que cumpla con los estándares requeridos. Tal y como se dispone en el sitio web oficial del Cuerpo Nacional de Policía y tal y como hemos recogido en el diagrama de flujos de la figura 14, el dispositivo móvil deberá adecuarse el estándar «ISO 14443, tipo A o B» cumplir con «ISO 14443 - Partes 1/2/3/4. Protocolo de transmisión T=CL»

Dicho conocimiento técnico sobre las versiones compatible para el uso del DNIe 3.0 podría complejizar o inhibir su uso.

La complejidad vinculada a las aplicaciones necesarias para hacer uso de la tecnología NFC no es precisamente tecnológica[44], asimismo, un mal acompañamiento a lo largo de todos los pasos a efectuar podría generar dificultades en los usuarios que quisieran hacer uso de los mecanismos.

En este caso la comunicación adecuada sobre los elementos a descargar indispensables para la puesta en marcha es clave.

Más allá de una comunicación adecuada, tambien deben tenerse en consideración aspectos de compatibilidad y es que, a la hora de instalar la aplicación de escritorio DNIeRemote tambien se deberá tener en consideración el sistema operativo y el tipo de unidad central de proceso (CPU) tal y como observábamos en el capítulo «4.1 Uso de los mecanismos de identificación electrónica» subapartado del DNIe.

Complementariamente, una vez descargadas ambas aplicaciones, estas deben vincularse. Para lo mismo se interponen dos medios – WIFI o USB -.

La vinculación por uno u otro método viene asociado a la necesidad de uso de otras tecnologías complementarías como el QR en el caso de la vinculación mediante WIFI o la necesidad de seguir una serie de especificaciones, en un orden concreto para llevar a término la vinculación mediante USB. Entre las especificaciones la de tener la «depuración de USB» habilitada.

[44] La complejidad principal identificada es la inconsistente, errónea y confusa información respecto a los requisitos y recursos necesarios para el uso efectivo del DNIe por medio de la tecnología NFC.

Respecto a los elementos que su naturaleza no es compleja en sí, pero que podrian complejizar el proceso de registro y puesta en marcha encontramos tres grandes barreras, las cuales se exponen a continuación:

4.5.3 Barrera 3. ¿Exceso de información? Información poco accesible y heterogénea

La falta de información al respecto de un proceso puede resultar perjudicial, esto podria dificultar o incluso inhibir el uso. Asimismo, el exceso de información – no mediada por un tercero experto - y la heterogeneidad en las diferentes fuentes, podría generar confusión e incertidumbre.

Tal y como se ha identificado a través del analisis de los diferentes mecanismos de identidad digital en el capítulo 4, este es el caso de la identidad digital en España. Vemos como más allá de la multiplicidad de mecanismos de identidad digital, tambien existen multiplicidad de fuentes – oficiales y no oficiales – de información en las que se explica su uso, los procesos de registro, los requerimientos para la puesta en marcha, etcétera.

- **Múltiples fuentes de información:** A través del analisis realizado, se han observado multiplicidad de fuentes alternativas en los diferentes mecanismos de identificación electrónica y firma digital. A modo de ejemplo tenemos el caso de la información al respecto del uso del «DNIe mediante antena NFC». Información relativa a esta la podemos encontrar en:
    - El sitio web «Portal del DNI electrónico, Cuerpo Nacional de Policía» en su apartado «Qué hace falta para utilizarlo» en el «Área de descargas» o en el «Manual completo de la aplicación sobre el funcionamiento y las opciones de configuración»
    - En otras páginas web sustentadas por otros organismos de la Administración Pública como la «GUIA DE REFENCIA DEL DNIE CON NFC» de la FNMT o el sitio web del «DNI Electrónico» del Portal de Administración electrónica.

Como se identificaba en el apartado 4.2 «¿Qué y dónde?: Mecanismos de interacción con la Administración Pública», sí que es cierto que se disponen portales oficiales para los diferentes mecanismos, no obstante, el usuario encontrará información al respecto de estos en múltiples lugares y a través de múltiples caminos.

- **Diferentes niveles de detalle.** Del mismo modo, gracias al analisis hecho en el capítulo 4, se ha podido evidenciar las diferencias en los niveles de detalle en las fuentes de información. A modo de ejemplo se podría decir que en una fuente el proceso puede estar compuesto por 3 pasos y en otra este mismo alcanza los 7 pasos.

Esto mismo lo volvemos a ejemplificar a través del caso del «DNIe mediante antena NFC». Una vez más, en el apartado «Qué hace falta para utilizarlo» se hace referencia a:

  - La instalación de un elemento hardware - Un dispositivo con NFC que cumpla el estándar ISO 14443, tipo A o B -.
  - Dos elementos “software”, uno de ellos «una aplicación»[45] y el otro un lector de tarjetas.

En este caso, un total de 3 pasos/requisitos a cumplir a fin de poner en marcha el DNIe mediante la tecnología NFC.

Por el contrario, en el caso de el «Manual completo de la aplicación sobre el funcionamiento y las opciones de configuración» ubicado en el área de descargas del mismo sitio web, se hace referencia a un total de 18 puntos y subpuntos en los que se detalla la puesta en marcha al completo, contemplando detalles imprescindibles para su uso efectivo.

Cabe resaltar dos aspectos:

[45] Como se ha comentado en diversas ocasiones no se hace referencia a un elemento identificativa de dicha Aplicación. Complementariamente, se hace referencia a la posibilidad de descargarla en Apple Store, siendo eso imposible pues no se ha desarrollado para dispositivos Apple y, por último, sin hacer referencia a que, dicha aplicación, trabaja en tándem con otra aplicación para el escritorio del equipo con el que se realizará el trámite.

- La complejidad para dar con la segunda fuente dado su ubicación poco intuitiva. Esta se encuentra en el subapartado DNIeRemote del «Área de descargas». Cabe destacar que el nombre de la aplicación DNIeRemote no se menciona previamente en ningún apartado, por ende, resulta dificil pensar que algún usuario llegase a dicho apartado por su propio pie.
- La existencia de fuentes de información con diferentes niveles de detalle e incluso información contradictoria o errónea, podría generar desconfianza, saturación o confusión en el usuario.

- **Falta de información e información contradictoria**. La existencia de más fuentes de información implica mayor esfuerzo para homogeneizar los contenidos y mantenerlos actualizados. Esto frecuentemente no se lleva a cabo y consecuentemente se encuentran informaciones o datos contradictorios entre unas y otras fuentes.

Siguiendo con el caso de «DNIe mediante antena NFC», en concreto se hablará de las aplicaciones necesarias para el uso efectivo de la tecnología y la vinculación entre los equipos necesarios. Como se ha comentado en algunos epígrafes más arriba, la comunicación de los elementos necesarios para la puesta en marcha del DNI mediante NFC no ha sido la más efectiva, y es que, como se ha comentado, para la vinculación efectiva entre el DNIe y los diferentes dispositivos, será necesaria la instalación de dos módulos que conforman la aplicación DNIeRemote.

Asi mismo en el sitio web «Portal del DNI Electrónico, Cuerpo Nacional de Policía» en el apartado «Que hace falta para utilizarlo» se hace referencia a las aplicaciones como «APLICACIÓN que utilice el DNI 3.0 para identificar al usuario y acceder a un servicio específico o para firmar electrónicamente un documento con igualdad jurídica que la firma manuscrita». En este caso vemos como de entrada no se nos hace referencia a ningun elemento identificativo de la aplicación, ni tampoco que esta deba ser complementada con una aplicación para escritorio.

Complementariamente, se hace referencia a la posibilidad de instalar a través de repositorios oficiales de aplicación «Para su instalación, proceda a descargar la

APLICACIÓN desde un repositorio oficial (Google Play/Aplicaciónle Store….)» sin hacer referencia una vez más a un elemento identificativo de la misma y, lo que es más, dando información errónea, pues dicha aplicación después vemos como no se ha desarrollado para sistemas operativos Apple y consecuentemente no se encuentra disponible en Apple Store.

Si se sigue indagando, se puede llegar al «Área de descargas», en concreto al apartado DNIeRemote– después sabremos, una vez entremos en dicho apartado, que el nombre de la aplicación matriz es ese – en el que se concreta la funcionalidad de la aplicación «La aplicación DNIeRemote aprovecha la tecnología NFC para convertir el dispositivo móvil en un lector del DNIe 3.0 conectado al PC, permitiendo así acceder a los servicios de la administración electrónica que requieren de autenticación con certificado digital, y realizar firmas digitales en documentos a través de las correspondientes aplicaciones»

En este caso, como podemos ver, todavía no ha hecho referencia a la existencia de una aplicación de escritorio que complemente a la aplicación para dispositivo movil – a la cual si se ha hecho referencia previamente – sino que se puede deducir pues, en el siguiente párrafo se hace referencia a «Esta aplicación funciona en conjunto con la aplicación para Android "Lector de DNIe para PC, usando el movil" que puede descargarse de Google Play, bajo el desarrollador cnp-fnmt.» en la que «esta aplicación» deduciblemente se trata de la aplicación de escritorio que complementa a la aplicación de movil a la que se refieren como "Lector de DNIe para PC, usando el movil".

En este caso, no se hace referencia a que la aplicación móvil pueda descargarse con Apple Store dado que no se ha desarrollado para sistemas operativos Apple, como se ha comentado previamente.

Complementariamente, una vez hemos descubierto la existencia de ambas aplicaciones, se nos hace referencia a que las mismas deberán vincularse. En algún punto se hace referencia a que dicha vinculación se hará a través de la conexión Wi-Fi.

> *«La aplicación se encarga de hacer que el móvil se comporte como un lector de tarjetas, y se comunica con la aplicación del computador personal a través de la conexión Wi-FI»*

Como veremos más adelante, en otras fuentes de información y como hemos visto en el subapartado del uso del DNI electrónico del punto 4.1, se expone que la conexión tambien podrá realizarse mediante USB, no solo mediante conexión WI-FI.

Siguiendo con la búsqueda de fuentes que expliquen detalladamente como puede ponerse en marcha todo este entramado de aplicaciones y conceptos vagamente descritos, encontramos en el mismo sitio web el «Manual completo de la aplicación sobre el funcionamiento y las opciones de configuración.»

Como se ha expuesto previamente, dicha fuente se trata de un documento más extenso en el que se detallan mucho más los procesos – aportando claridad en relación con algunos conceptos y procederes-.

Como se ha podido observar a través del analisis del documento, este viene a contradecir y/o concretar información que previamente se había observado en otras fuentes:

- En dicho manual se especifica que, DNIeRemote, está conformado por dos módulos – dos aplicaciones – una para el dispositivo móvil y otra para escritorio, cosa que previamente no se había mencionado.
- Complementariamente, se especifica que la aplicación para escritorio es compatible con Linux/Windows y la aplicación para dispositivo móvil, compatible con Android, desmintiendo la posibilidad de descargarlo en dispositivos Apple.
- En este caso se hace referencia a la aplicación para dispositivos móviles como «DNIeSmartConnect» mientras que en otros lugares se hacía referencia a la aplicación bajo el nombre de "Lector de DNIe para PC, usando el movil".
- Como se ha comentado previamente, la vinculación entre ambas aplicaciones tambien puede darse a través de USB y es en el presente manual que se explicita.

Mas allá de las incongruencias identificadas, no es hasta dar con el presente manual que el usuario podrá tener información de especificaciones técnicas a cumplir sin las cuales no podrá hacer uso efectivo de dicha tecnologia.

Al fin y al cabo, que existan multiplicidad de fuentes a las que acceder para informarse implica:

- Para la administración: mayor esfuerzo para mantenerlas actualizadas; mayores esfuerzos por homogeneizar la terminología utilizada, mayor esfuerzo con contemplar el mismo nivel de detalle en todas las fuentes disponibles asi como evitar la información contradictoria.
- Para el administrado: sin obviar el hecho de que tener múltiples puntos de acceso podría ser beneficioso para ocasiones en las que una de las fuentes no estuviese disponible, el tener acceso a multiplicidad de fuentes con diferentes informaciones contenidas en si (en terminos de detalle, terminología u otros aspectos) podría llegar a generar confusión e incertidumbre por sobreinformación o por recibir información contradictoria.

  Complementariamente, en el canal digital no tenemos a un intermediador que nos disipe la duda que tenemos en el momento, generando esto frustración y rechazo.

Por último, vinculado con la falta de información y/o dispersión de esta, vemos cómo podemos encontrar multiplicidad de fuentes que nos dan información al respecto de un mecanismo, pero no una única en la que se nos comunique del conjunto de procesos a realizar, de la visión global del proceso. Esto ayudaría al usuario a contextualizarse, a saber, que se le requerirá, en qué punto está y cuanto le queda para acabar el proceso de registro y puesta en marcha de los mecanismos.

Con salvedades, pue en el caso del certificado digital de la FNMT-CRM el usuario si puede entender de manera rápida y visual, cuáles son los pasos por cumplir y en cual se encuentra en cada momento.

4.5.4 Barrera 4. Procesos largos e interrumpidos y fragmentados

Otra de las complejidades o elementos que no favorecen la usabilidad de los mecanismos de identificación digital son los largos, interrumpidos y fragmentados procesos, tal y como hemos podido observar a través de los

diagramas de flujo. Podríamos destacar lo poco operables que son en algunos casos. Los siguientes subcapítulos describen las ineficiencias identificadas propias de los procesos.

- **Extensión**

Ya hemos podido observar a través del analisis realizado en apartados previos, asi como a través de los diagramas de flujos, la extensión de los procesos de registro y puesta en marcha de los diferentes mecanismos. Asimismo, tal y como hemos podido analizar, en todos los procesos observamos que el usuario debe llevar a cabo un total de entre 13 a 29 pasos en función del tipo de mecanismos que quiera obtener.

Tabla 3.

Extensión de los procesos de puesta en marcha los diferentes mecanismos de identidad digital en España

	Clave PIN				Clave permanente				Certificado digital		DNIe	
	Registro básico		Registro Avanzado		Registo básico		Registro Avanzado				Presencialmente	
	Videollamada	rta de invitac	esencialmer	DNIe/certificado	Videollamada	Carta de invitación	Presencialmente	DNIe/certificado	ersonalmente mediante softwar	DNIe	Mediante contacto	Sin contacto (NFC)
Pasos	**24**	**28**	**21**	**22**	**25**	**29**	**21**	**23**	**26**	**18**	**13**	**17**
Registro	18	22	15	16	18	22	14	16	23	15		
Puesta en marcha	6	6	6	6	7	7	7	7	3	3	13	17

Fuente: Elaboración propia a partir de los respectivos sitios web.

En el caso de los procesos de Cl@ve PIN, la expansión puede variar en función del tipo de registro por el cual se obtiene, esto previo más los pasos que requiere la instalación de la aplicación «clave PIN» indispensable para hacer uso del mecanismo.

De igual modo, en el caso de cl@ve permanente, la extensión varía en función de la tipologia de registro, asimismo los pasos que requiere la puesta en marcha protagonizada por la activación del mecanismo no varían.

En este caso vemos que, por lo que respecta a la extensión de los procesos no hay gran diferencia entre los registros básico y avanzados, tanto en cl@ve PIN como en cl@ve permanente. Un aspecto algo contraintuitivo dado que la obtención de los mecanismos cl@ve a través del registro avanzado aportará mayores credenciales que si se obtienen a través del registro básico.

En el caso del certificado digital sí que observamos diferencia notable entre la extensión por obtenerlo a través de cita presencial o a través de DNIe (opción

solo disponible si previamente el usuario ha puesto en marcha el DNIe por los medios habilitados)

Por último, en los casos del DNIe vemos que comparativamente los procesos no son tan extensos. Asimismo, la complejidad o coste de cada uno de los pasos es superior. No solo por la complejidad en si de lo que implica cada uno de los pasos – complejidad técnica derivada de la instalación de múltiples elementos complementarios - sino derivado de otros elementos como la dificultad de acceso a la información, lo fragmentada que se encuentra los errores en la redacción o la información inexistente o poco accesible.

Por ende, vemos como la extensión del proceso no determina la complejidad de este, sino que se dan otros aspectos que dificultan el entendimiento, registro y puesta en marcha de estos.

Entre alguno de los elementos que complejizan el proceso encontramos las subtareas o el nivel de fragmentación del proceso.

- **Subtareas**

Por lo que respecta a las subtareas, el 100% de los mecanismos presentan. Es decir, como parte del proceso se contemplan subprocesos necesarios para llevar a cabo el registro y/o puesta en marcha. Algunos ejemplos de los mismo serían:

- Introducir un código enviado al dispositivo móvil por SMS o al correo electrónico.
- Llevar a cabo el proceso de activación de cl@ve permanente tras el registro
- Los procesos de cita previa del sistema cl@ve y certificado digital. Los sitios web de estos, solo cuentan con buscadores de oficinas cercanas. Asimismo, no se puede pedir cita a través de esto, son enlaces meramente informativos.
- Búsqueda, descarga e instalación de elementos externos como los programas complementarios necesarios para la puesta en marcha de los diferentes mecanismos. Ejemplos de esto son los drivers o módulos criptográficos para hacer uso del DNIe mediante lector de tarjetas, las aplicaciones DNIeRemote y «DNIeSmartConnect» para hacer uso del

DNIe mediante tecnología NFC, la necesidad de instalación de autofirma y los certificados raíces en el caso del certificado digital o la adecuación de navegadores u otros programas como Java.

Complementariamente, la asistencia que se le da a los usuarios para la realización de dichas subtareas es vaga, en algunos casos no describiéndose el camino para la consecución de estos ni la ubicación de los elementos requeridos. Ejemplo de esto previo es el proceso de activación de cl@ve permanente, que como se ha comentado en apartado anteriores dar con el sitio web de activación, no es intuitivo.

Esto es determinante, frecuentemente encontramos que se demanda la instalación de un elemento para poner en marcha un mecanismo determinado, asimismo, no se explica al usuario como hacerlo. En su defecto, se podría llegar a encontrar algun otro recurso si el usuario busca por el navegador. En todo caso no se dispone junto al punto en el que se está requiriendo dicha acción.

- **Fragmentados**

Respecto a la parcialidad o fragmentación de los procesos, vemos como de entrada el usuario no podrá realizar el proceso de forma conveniente, resolviendo la inquietud que le ha llevado a adquirir uno de los mecanismos de identidad digital.

Se observa que, para hacer efectivo el registro y/o puesta en marcha de los diferentes mecanismos, el usuario deberá acceder a otros sitios web o, en su defecto, ponerse en contacto con la administración de turno para hacer cierto trámite.

Esto se observa principalmente en los mecanismos en los que se requiere de presencialidad y, por ende, hay que pedir cita previa - mecanismos de certificado digital y sistema cl@ve -. En ambos se ofrecen soluciones meramente informativas. Esto es, el usuario no podrá pedir cita a través de la plataforma, sino que tiene que valerse de los medios de contacto habilitados por cada una de las oficinas.

Tambien lo vemos en los casos de cl@ve permanente. Para dicho mecanismo se requiere de la activación del usuario una vez este se haya registrado por los

diferentes caminos habilitados. En este caso vemos como los servicios de activación o el enlace directo al sitio web a través del cual poderla llevar a cabo, no se contemplan en ninguno de los apartados en los que si se menciona la activación.

Como comentábamos, este se menciona en diversos sitios:

- Apartado de «¿Qué es Cl@ve?» del capítulo de «cl@ve» dice asi «Una vez que te hayas registrado y hayas activado estas claves de acceso…»
- Apartado de «¿Cómo puedo registrarme?» del capítulo de «registro» dice asi «… acceder a los sistemas de activación de contraseña del sistema Cl@ve permanente»
- Apartado de «¿Qué es?» del capítulo de «cl@ve permanente» dice asi «Para acceder al proceso de activación es necesario que previamente te hayas registrado en el sistema»

Pero en ninguno de los casos vemos enlace de acceso al sitio web donde llevar a cabo el proceso de activación – indispensable para la puesta en marcha del mecanismo – así como tampoco se dispone un sitio web en el que se contemplen todos los pasos indispensables para el proceso, en el que se contemple dicho paso, entre otros.

Por el contrario, el usuario que haya leído todos los textos dispuestos en los diferentes sitios web, deducirá que debe activar la cl@ve para hacer uso de esta.

El apartado en el cual se dispone un enlace directo a los servicios de activación se encuentra en «Características de la contraseña»[46] del apartado «cl@ve permanente» tal y como vemos en el diagrama de flujos de la figura 9.

En su defecto, al buscar en el navegador «Activación cl@ve permanente» el usuario podría acceder al mismo sitio web.

Por lo que respecta a las modalidades de tramitación de los procesos, el 84%[47] se pueden llevar a cabo en remoto. Esto es debido a que se proponen

[46] Véase: https://clave.gob.es/clave_Home/Clave-Permanente/Procedimientos.html

[47] Se contabilizan como modalidad en remoto tanto las opciones de DNIe mediante contacto como DNIe sin contacto mediante tecnología NFC. Esto es, dada la obligatoriedad de disponer del Documento Nacional de Identidad, se asume que el usuario ya dispone de uno y que por ende la acreditación presencial de la identidad ya se ha efectuado.

alternativas de acreditación de la identidad del usuario en remoto, ya sea mediante DNIe o certificado digital – procesos en los cuales ya se ha acreditado la identidad de manera presencial – como a través de soluciones en remoto como el registro mediante videollamada.

Las soluciones que si o si implican presencialidad son las del registro en oficina para el sistema cl@ve y la personación en una oficina para el caso del certificado digital.

De entre los procesos que implican presencialidad obligada deberían tenerse en consideración los tiempos de espera para la cita previa asi como el lugar de las oficinas disponibles.

- **Elevada dependencia del móvil**

Por último, al respecto de los elementos que complejizan el proceso cabe destacar la elevada dependencia del teléfono, lo cual engorda el número de subtareas a realizar y fragmenta el proceso al tener que depender de otro elemento externo para finalizarlo. Dicha dependencia la observamos a través de los diferentes diagramas de flujo a través de los requerimientos de doble verificación u OTP.

De acuerdo con criterios de seguridad, frecuentemente es necesaria una doble autentificación – lo que hemos conocido como OTP - la cual suele implicar el uso del dispositivo movil del interesado. Asimismo, no puede predecir con anticipación cuándo se demandará, pues no se explicita en ningun lugar.

Lo impredecible de la demanda puede generar insatisfacción o malestar. Complementariamente, no es infrecuente la demanda de la doble verificación, sino que el 77,5% de los trámites de la muestra pueden requerir del dispositivo móvil a lo largo del proceso (*¿Son claros los trámites digitales?*, 2022, pg. 71).

> *“No hay forma de predecir cuándo se le va a solicitar a la ciudadanía esa validación extra” (¿Son claros los trámites digitales?*, 2022, pg. 71)

Dicha previsión si puede tenerse cuando se opta por autentificarse mediante Cl@ve PIN, mecanismo de identificación que requiere del uso de una aplicación móvil. Asimismo, en el resto de las ocasiones el ciudadano no puede deducir si se le demandará una doble autentificación que requiera el tener a mano un

dispositivo móvil cuando el trámite no se estaba llevando a cabo a través de dicho dispositivo.

A continuación, se categorizan y codifican todos los elementos de complejidad identificados a lo largo del analisis. Para lo mismo, se han creado las categorias de complejidad conceptual, técnica, informacional y procedimental para cada uno de los mecanismos analizados.

La categoria «conceptual» alude a todas las cuestiones vinculadas con el entendimiento del ecosistema de identidades digitales asi como de los diferentes actos habilitados: identificación electrónica y firma digital. En dicha categoría se ven involucrados todos los mecanismos pues todas forman parte del ecosistema de identidades digitales en España y todos pueden verse involucradas en la confusión entre los actos de identificación electrónica y firma digital.

Por lo que respecta a la categoría de complejidades técnicas, en este caso tecnológicas, es el DNIe quien destaca al ser el mecanismo que requiere de mayores conocimientos técnicos para su puesta en marcha, desde los requerimientos técnicos de algunos de sus elementos asi como el número de programas a instalar.

Por lo que respecta a la tercera categoría, la que alude a las complejidades generadas por una incompetente comunicación de la información necesaria, vemos como, indistintamente del mecanismo, se identifican problemas por lo que se refiere a la información pública necesaria para el registro y puesta en marcha.

Por último, se alude a las complejidades derivadas de la naturaleza de los procesos, extensos en su mayoría, presentando múltiples subtareas a realizar, asi como como la fragmentación o incompletitud de estos.

Figura 15.

Cuadro resumen de los elementos de complejidad de la identidad digital española

Fuente: Elaboración propia a partir de los datos de la investigación

5 COMPARATIVA INTERNACIONAL

En el siguiente capítulo, sobre la base de que la identidad digital podría ayudar a mitigar el desajuste entre oferta y demanda de servicios públicos, analizaremos las soluciones de identidad digital de países europeos que, perceptiblemente, podrían ayudar a superar las barreras identificadas en el caso de la identidad digital española.

El propósito del analisis de las soluciones de identidad digital en otros países se da pues, de acuerdo con los informes previamente revisados[48] vemos como se produce cierta correlación entre países con un nivel de penetración social más elevado y un mayor desarrollo en materia de identificación electrónica. Sería interesante importar dichas maneras de hacer y ver el impacto que tendría en terminos de uso de los servicios públicos digitales.

De entrada, se analizarán los países que llevan delantera por lo que se refiere a la identidad digital, en este caso los pioneros en la materia son Islandia, Dinamarca, Estonia, Finlandia, Noruega, Malta y Lituania (*e-government* Benchmark, 2022) así como otros países en los cuales presenten buen desempeño en la materia.

El analisis de sus identidades digitales nos ayudará a hacer contrapropuestas concretas a las barreras identificadas en el caso español.

5.1 Contrapropuesta a la barrera 1: Simplificación del ecosistema de la identidad digital

Como habiamos apuntado previamente, la identidad digital en España se traduce en dos actos, los de identificación electrónica y firma digital (C3), los cuales, a su vez, los vemos reflejados en diferentes mecanismos de identidad digital (C2) de la administración pública. Existen aquellos con los cuales solamente se puede llevar a cabo la identificación electrónica, con los que se puede firmar digitalmente y con los que se pueden llevar a cabo ambos actos.

[48] European Comission et al. (2022) eGovernment Benchmark 2022 y European Commission. (2022). DESI - Digital Public Services 2022.

Tener que ser conocedor de para que sirve cada mecanismo – identificación o firma – asi como saber las diferencias entre los diferentes mecanismos existentes, complejiza la comprensión de algo tan sencillo como lo sería la exhibición del DNI ante un tercero. Esto abre la veda a ulteriores dudas como ¿Para qué sirve cada uno de los mecanismos? ¿Qué les diferencia? ¿Cuál me conviene más para un determinado trámite? (C1). Y un sinfín de preguntas que surgen al existir diversas opciones.

La barrera y potencial brecha que puede generar es enorme, el no entender el ecosistema de la identidad digital puede generar desafección, rechazo, o incluso pasividad ante los mismos, el "sí puedo evitarlo, lo evito"

En este caso, lo que se observa en el panorama internacional es que la identidad tradicional - una sola – se traduce a otra única identidad digital (C1) que habilita la identificación y firma digital del usuario (C2). En su defecto, observamos casos en los que efectivamente tienen más de un mecanismo de acceso a la administración pública pero siempre y cuando estos aporten un valor funcionalmente distinto.

En el caso de Dinamarca, actualmente disponen del «MetID», la tercera generación de *eID* y la cual, se erige como identidad digital única de todos los daneses y a partir de la cual, los ciudadanos daneses pueden identificarse y firmar convenientemente.

> *"Aquí, el sector financiero danés y las autoridades públicas trabajaron en estrecha colaboración para emitir a casi todos los residentes una identidad digital única que coincida con su número de registro civil danés."* (Agencia de Gobierno Digital Danés, 2023)

De igual modo, observamos el caso holandés, los cuales también apuestan por una identidad digital única, el DigiD[49], mecanismo que te permite identificarte a la hora de hacer tramites online.

En la misma línea observamos en caso islandés[50]. Estos, de igual modo, cuentan con un sistema de identificación electrónica único que "pueden utilizarse tanto

[49] Véase: https://www.digid.nl/en/what-is-digid
[50] Véase: https://island.is/en/electronic-id

para fines de identificación como de firma, en particular" (Gobierno Islandés, 2023). Este sistema de autentificación puede utilizarse a través de tres modalidades, en formato físico a través de una tarjeta con lector, y a través de opciones móviles, una de ellas vinculada a la tarjeta SIM del usuario y otra en formato aplicación, y, por ende, usable en cualquier dispositivo indistintamente de la SIM que contenga.

Este modelo, tambien los observamos en los caso estonio y lituano, que a continuación detallamos.

El modelo de identidad digital de Estonia ofrece tres alternativas de acceso, en este caso serían la ID-card, Mobile ID y Smart ID

El ID-card – homólogo del DNI en España – es un documento físico obligatorio para todos los ciudadanos estonios, asimismo este puede utilizarse a modo de medio de identificación digital para el acceso a todos los servicios públicos digitales. Complementariamente, se ofrecen las alternativas móviles «Mobile ID» - vinculada a la tarjeta SIM del dispositivo - y «Smart ID» - la opción usable solamente en el dispositivo en el que se ha instalado la aplicación - es decir de acceso a través de dispositivos inteligentes como las que hemos observado en el caso islandés y veremos en el caso lituano.

Parecido al caso estonio encontramos el caso lituano. Los ciudadanos disponen de diversos mecanismos de identificación electrónica. De igual modo al modelo estonio y español, en Lituania disponen del Documento de Identidad Nacional «*Lithuanian National Identity card (Eid/ATK)*» este puede utilizarse para la identificación y la firma electrónica. Complementariamente, tambien disponen del Mobile ID[51] y Smart ID[52] similares a los observados en el caso estonio e islandés.

Lo que observamos del conjunto de soluciones presentadas es que:

- Los usuarios pueden identificarse electrónicamente asi como firmar digitalmente sin la existencia de limitaciones en este sentido o la existencia de mecanismos orientados a la identificación y otros a la firma.

[51] Disponible en: https://www.skidsolutions.eu/en/services/digital-identity/mobile-id
[52] Disponible en: https://www.skidsolutions.eu/en/services/smart-id/

Los mecanismos habilitados son holísticos en este sentido facilitándose la autentificación al usuario. (C2 y C3)

- Un único mecanismo de identidad electrónica. En su defecto, un número más acotado de soluciones de identificación electrónica lo cual podria facilitar el entendimiento de las existentes, asi como de cuál es la más adecuada para determinados propósitos. (C1)
- Soluciones de identificación digital funcionalmente distintas. En el caso danés vemos como solo existe una solucion de identificación digital, con lo cual no habría confusión con otros mecanismos y en los casos de las repúblicas bálticas de Estonia y Lituania e Islandia, vemos como existen soluciones de escritorio, es decir para utilizar con PC y otras opciones móviles para utilizar en dispositivos inteligentes. Mecanismos funcionalmente diferentes, que por sí mismo aporten un valor público distinto al resto. (C1, C2 Y C3)

5.2 Contrapropuesta a la barrera 2: Simplificación técnica para mitigar la brecha digital

Por lo que respecta a las barreras técnicas identificadas, se destacan las tecnológicas. En el caso de la identidad digital en España se han identificado, en algunos de los mecanismos, requisitos altamente técnicos (T1) a nivel tecnologico (requisitos hardware y software), asi como la instalación de ulteriores programas necesarios para la puesta en marcha y uso de los mecanismos (T2)

Al respecto del requerimiento altamente técnicos (T1), se destacan:

- El caso del DNIe mediante lector de tarjetas: vemos como para hacer uso del DNIe por dicho medio, entre otros, necesitaremos disponer de un lector de tarjetas con las siguientes especificaciones tecnológicas:
    - *El estándar ISO-7816 (1,2 y 3)*
    - *Soporta tarjetas asíncronas basadas en protocolos T=0 (y T=1)*
    - *Soporta velocidades de comunicación mínimas de 9.600 bps.*
    - *Soporta los estándares:*
        - *API PC/SC (Personal Computer/Smart Card)*

En este caso, es inevitable demandar un lector de tarjetas con dichos requerimientos tecnológicos a fin de que este sea compatible con la tarjeta en sí, asi como para garantizar seguridad en su uso. No obstante, dejar en manos del ciudadano la decisión de dirimir entre infinitas opciones disponibles en el libre mercado, satura y no aporta la seguridad que requiere el trámite a realizar.

En este caso vemos como otros países proponen alternativas a este modo. El caso de ejemplo de nuevo es el estonio.

En el sitio web oficial de la identidad digital estonia – portal en la que se ofrece toda la información necesaria sobre los diferentes mecanismos de identificación digital – en el apartado de «lector de tarjetas» encontramos un listado de lectores de tarjetas testeados[53] y compatibles con su «ID card». Con esta opción limitamos la inseguridad que pueda sentir el ciudadano asi como reducimos la incerteza del ciudadano al acotarle el número de alternativas igualemente viables.

De igual modo, tambien lo vemos en el caso islandés para su alternativa física de identificación electrónica. En este caso, dicha alternativa tambien funciona mediante una tarjeta física a la cual se accede mediante un lector de tarjetas. Dicho lector de tarjetas a pesar de no ser provisto por las autoridades públicas islandesas, lo proveen las entidades bancarias del país.

Otra de los elementos complejos identificados, es la instalación de múltiples elementos técnicos (T2), principalmente en el caso del DNIe en ambas versiones – con contacto y sin contacto (NFC) – para el cual encontramos los requerimientos de instalación de drivers y módulos criptográficos para el uso del lector de tarjetas, así como la instalación de ambas aplicaciones DNIeRemote y DniSmartConnect.

Por lo que respecta a la necesidad específica de instalación de un elemento concreto, sería deseable que el propio portal o sitio web de dicho mecanismo de identidad digital identificase inequívocamente el elemento a instalar, más teniendo en cuenta que gracias a la digitalización basta con enlazar dicho sitio web con el sitio web en el que descargar el elemento requerido. Lo vemos en el

[53] Véase: https://www.id.ee/en/article/useful-information-about-smartcard-readers/#tested-card-readers_1

caso de la identificación mediante Aplicación en el caso islandés, aplicaciones para las cuales se dispone un enlace directo a los repositorios oficiales[54] de Google Play y Apple Store.

Por último, tambien encontramos situaciones en las cuales, al usuario se le requiere la instalación de ulteriores programas (T2) necesarios para la puesta en marcha y uso de los diferentes mecanismos y que estos sean compatibles con el equipo en el que se van a utilizar (T1). Este es el caso de la instalación del software para hacer uso del Certificado digital[55], el caso de la descarga de la aplicación de escritorio DNIeRemore para hacer uso del DNIe electrónico mediante la tecnologia NFC[56] o el caso de los módulos criptográficos[57] para hacer uso del DNIe mediante lector de tarjetas, entre otros. En todos los supuestos será el usuario quien tenga que dirimir que versión instalar en función del sistema operativo y el tipo de unidad central de proceso (CPU) de su equipo.

En este caso, para prevenir incompatibilidades y complicaciones, se propone la autoidentificación del software a instalar. Una vez más proponemos la solución del gobierno estonio. Para la puesta en marcha del «ID-Card», tambien sería necesaria la instalación de un software en adecuación con sistema operativo del equipo, asimismo en este caso, el propio sitio web identifica automáticamente el sistema operativo y el tipo de unidad central de proceso del equipo en el que se va a instalar. Esto evita que sea el usuario quien tenga que determinar que versión de software debe instalar. De igual modo, en el mismo sitio web se explicitan los pasos a seguir para instalarlo de manera fructífera.

En este caso, mediante la comparación con los diferentes casos analizados, lo que se pretende es evidenciar de manera sencilla como reducir la complejidad y simplificar el proceso al ciudadano. Esto es, no se propone eliminar la necesidad de lector de tarjetas, la necesidad de instalación de una aplicación o la del software necesario para la puesta en marcha de los mecanismos, sino que se

[54] Véase: https://island.is/en/electronic-id/audkennisaplicaciónid

[55] Véase: https://www.sede.fnmt.gob.es/descargas/descarga-software/instalacion-software-generacion-de-claves

[56] Véase: https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_1015&id_menu=65

[57] Véase: https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_300&id_menu=15

proponen soluciones automatizadas, aclaratorias y sencillas que orientan al usuario.

Lo que observamos de acuerdo con el análisis realizado es:

- La necesidad de proponer soluciones más automatizadas. Esto no quiere decir que deban suprimirse elementos como el lector de tarjetas – y sus respectivos requerimientos técnicos – ni la eliminación de los softwares para hacer uso de los mecanismos que los requieran o suprimir las aplicaciones móviles necesarias. Por el contrario, lo que se observa es la simplificación del camino haciendo uso de:
    - La tecnología: en los casos en los que el usuario debe decidir entre que versión de software debe descargar, vemos como en otros casos es el programa el que identifica la versión adecuada para el equipo en el que se va a descargar.
    - La comunicación: en los casos en los que simplemente en necesario tener acceso a la información adecuada, serían los sitios web como fuente de información los que tendrían que estar estructurados de tal modo que el usuario fuese navegando convenientemente a la part que realiza los pasos necesarios para la puesta en marcha de los mecanismos.

5.3 Contrapropuesta a la barrera 3: Depuración conceptual y homogeneización de las fuentes de información

Como se puede deducir, la existencia de mayor número de mecanismos de identidad digital implica la existencia directa de más fuentes de información que aludan a las mismas. Este es el caso español, como hemos podido ver existen diversos mecanismos provistos por diferentes autoridades.

El DNIe está gestionado por el Cuerpo Nacional de Policía, el Certificado digital por la FNMT-CRM o el sistema cl@ve por la Agencia tributaria. Cada uno de los mismos habilita sus respectivos sitios web para los mecanismos de identificación electrónica gestionados. Es decir, de entrada, el usuario no puede tener una idea completa del ecosistema de soluciones disponibles, sino que, de manera

reactiva[58] o parcheada, el usuario irá conociendo el conjunto de identidades existentes en los múltiples sitios web (I1).

En el caso de otras soluciones de identidad digital analizadas en el marco internacional vemos como, el conjunto de soluciones disponibles se encuentra concentradas en un mismo directorio. Esto permite dar a entender el ecosistema de soluciones asi como una entrada conveniente e intuitiva al conjunto de mecanismos disponibles como es en el caso estonio, en el cual encontramos un sitio web común relativo a la identidad digital[59] en las cual podemos encontrar los diferentes mecanismos habilitados – ID-card, mobile-ID y Smart -ID – con toda la información necesaria para ponerlos en marcha y hacer uso de ellos. Lo mismo lo vemos en el caso islandés es su sitio web island.is[60] en el que de igual modo vemos las diferentes soluciones ofrecidas en materia de identificación digital «Electronic ID on a smartphone», «Electronic ID card» y «Auðkenni authentication aplicación»

Asimismo, tambien vemos como, para un mismo mecanismo de identificación no encontramos toda la información necesaria en un mismo sitio web (I1). Este es el caso del DNIe, tanto la puesta en marcha mediante lector de tarjetas como mediante la tecnologia NFC. En este caso volvemos a encontrarnos con la misma barrera, la existencia de múltiples fuentes de información[61], con diferente información asi como diferentes niveles de detalle y a la cual no se llega de manera intuitiva.

Sería conveniente que en un solo sitio web de la entidad que lo gestiona y emite- en este caso el Cuerpo Nacional de Policía – se encontrase toda la información, de manera ordenada e intuitiva.

Esto sí, lo encontramos más resuelto en mecanismos de identificación del estado español como serían en el sistema cl@ve y certificado digital de la FNMT-CRM,

[58] El usuario se ve forzado a utilizar un mecanismo de identificación electrónica porque se le requiere para la realización de un trámite.
[59] Véase: https://www.id.ee/en/
[60] Véase: https://island.is/en/authentication-system
[61] Para el DNIe encontrábamos información en el apartado «Que hace falta para utilizarlo» asi como en más detalle en el informe «GUIA DE REFENCIA DEL DNIE CON NFC»

al menos por lo que respecta al registro en el sistema y en la instalación de los medios necesarios.

A nivel internacional, encontramos las soluciones del:

- MitID danés para el cual encontramos su propio sitio web[62] en el cual se expone toda la información necesaria de las alternativas para obtenerlo y de las opciones para usarlo.
- IDcard estonio, del cual obtenemos información en el sitio web de la identidad digital en el país, con un apartado específico[63] para dicho mecanismo y en el cual, paso a paso de nos muestra cómo poner en marcha nuestra identificación digital, contemplando la instalación del software necesario, la adecuación del navegador, asi como información respecto a «RIA DigiDoc mobile aplicaciónlication» su alternativa móvil.
- National Cards belga, para el cual se dispone un sitio web específico[64] en el que se guía al usuario a través de las diversas pestañas en las cuales podrá descargar e instalar el software necesario, una guía de como instalarlo, explicado visualmente.

Estos, entre otros casos, reflejan con sencillez la manera de organizar toda la información necesaria relativa a un mecanismo de identificación electrónica, de manera procedimental, clara y accesible.

De estos previamente expuestos y otros como el de la identidad digital islandesa u holandesa, tambien recogemos algunas soluciones que podrían ayudar a evitar problemas generados por la falta de información. Esto es la comunicación del proceso global, es decir, de todos los pasos requeridos para el registro y la puesta en marcha de los mecanismos.

En el caso holandés, en el proceso de obtención de su identidad digital «digitD», el usuario puede ser consciente del proceso completo con una revisión en diagonal del propio sitio web[65], en el cual, gráficamente se explicitan cada una de las fases por las que el usuario deberá pasar a fin de obtener el mecanismo.

[62] Véase: https://www.mitid.dk/en-gb/
[63] Véase: https://www.id.ee/en/article/install-id-software/
[64] Véase: https://eid.belgium.be/en/how-install-eid-software
[65] Véase: https://www.digid.nl/en/apply-and-activate/apply-digid/

Asimismo, sin ir más lejos, esto mismo lo vemos en el caso del certificado digital de la FNMT-CRM. Tal y como podemos observar en su sitio web se detalla gráficamente cuales son las cuatro grandes fases para realizar de manera secuencial.

Por lo que respecta a la existencia de múltiples fuentes de acceso (I1) a la información, como se ha comentado previamente, se deberá poner más empeño y esfuerzo en el mantenimiento y actualización de estas.

De las barreras identificadas relacionadas con la gestión de la información, tanto en la existencia de fuentes con distintos niveles de detalle (I2) asi como falta de información o información contradictoria (I3) para la puesta en marcha de los mecanismos deseados, sería pertinente la optimización de las fuentes para evitar todas las externalidades negativas expuestas previamente, es decir la concentración de toda la información en una única fuente de información.

En su defecto, dicha barrera podría mitigarse mediante la homogeneización de la información a disposición en las distintas fuentes de información. De entre los aspectos a homogeneizar se destacan los siguientes:

- A destacar la importancia de llevar a cabo una depuración conceptual u homogeneización terminológica (C7). Esto es, llegar a terminos sobre cuál debería ser el nombre de un elemento en concreto y asegurar que será este término será el que se utilizará en todas las webs institucionales. Este podría ser el caso del «certificado digital» el caso más llamativo y controvertido. En este caso, se explicita en la propia web el hecho de que existen diversos terminos para referirse al mismo.
- En la línea vemos que la existencia de múltiples fuentes (I1) propicia la existencia de que las fuentes presenten diferentes niveles de detalle. La optimización de fuentes y concentración en una única haría del proceso de obtención uno más conveniente y fructífero, potenciando la obtención y uso de los mecanismos de identidad digital.
- Asimismo, mediante la homogeneización o supresión de fuentes de información se eliminaría la información contradictoria y podrían llegar a mitigarse los errores identificados en materia de comunicación.

Por último, por lo que respecta a la comunicación del proceso, se destaca la importancia de la contextualización del usuario en proceso, para gestionar de manera adecuada las expectativas, evitar frustración y hacerle consciente del conjunto de aspectos que tendrá que cumplir a fin de obtener el mecanismo de identidad digital que requiera.

5.4 Contrapropuesta a la barrera 4: Procesos transversales y menos exigentes

Por último, se ha analizado la naturaleza y disposición de los procesos de registro y puesta en marcha de algunas identidades digitales en el panorama europeo.

En el capítulo sobre las barreras identificadas en el caso de la identidad española, se destacaban algunos aspectos como:

- La extensión de los procesos (P1)
- La necesidad de llevar a cabo múltiples subtareas (P2)
- La fragmentación o incompletitud de los procesos (P3)

En el caso de la identidad digital española, la existencia de múltiples identidades digitales, *a priori*, funcionalmente distintas, implica que posiblemente el usuario no deba adquirir un solo mecanismo - con su proceso respectivo -, sino que, quizá este deba adquirir otro que cuente con otras características indispensables para el proceso que quiera tramitar en ese preciso instante.

Por ende, dada la naturaleza del ecosistema de identidad digital en España, el usuario no solo se verá abocado a un proceso de “x” pasos, sino que más bien a dos procesos con sus pasos respectivos.

Asimismo, independientemente de los mecanismos que un usuario pudiese llegar a necesitar, los procesos de otras identidades digitales analizadas a nivel europeo presentan procesos menos extensos (P1). Y vemos como más allá de la extensión más reducida de los procesos, se observan menos subtareas o se tratan de soluciones *end to end*[66](P3).

[66] Entendemos la expresión *end to end* como referente a un proceso completo, que va de principio a fin.

Por lo que respecta a las subtareas a realizar, efectivamente si, tambien se observan. No obstante, no en la misma medida.

En algunos de los mecanismos analizados como «mitID» o «digiD» no se requiere por ejemplo de ulteriores programas (P2) para poner en marcha los mecanismos, sino que basta con la cumplimentación de formularios con datos intuitivos y familiares para el usuario (nº de identificación personal, número de telefono, fecha de nacimiento, etcétera).

En su defecto, en los casos en los que, si se requiere, se opta por alternativas automatizadas como lo hemos visto ya en el caso estonio, en el que, sí que se debe descargar algun programa, así mismo el propio sistema identifica el sistema operativo del equipo en el que se instala. Es decir, se orienta y acompaña al usuario para cumplir con todos los requisitos demandados.

Otro aspecto que ayuda a simplificar el proceso es la posibilidad de poder comenzar y finalizar trámites de manera completa (P3). Un ejemplo significativo son las opciones para pedir cita previa. En los casos de cl@ve y certificado digital españoles, como se ha comentado en capítulos anteriores, las aplicaciones de cita tienen una funcionalidad meramente informativa. Conveniente sería la creación de una plataforma a partir de la cual poder pedir cita previa, sin tener que recurrir a canales de contacto externos y no homogeneizados. Si bien podría tomarse como ejemplo el caso de la cita previa en el caso del DNI español u otras opciones como la del caso danés con su plataforma automatizada y homogeneizada para la concertación de cita previa en «mitID».

Por último, como elemento que aportaría fluidez al proceso, sería interesante que el usuario tuviese acceso intuitivo a los diferentes pasos. Cogiendo como referencia el caso de la activación de cl@ve expuesto en capítulos previos, vemos como el usuario no puede identificar de manera conveniente el sitio web en el que activar su clave. Diferente es el caso de la activación de digiD. De igual modo, en el caso danés se le proporciona al usuario un código de activación que debe ser ingresado en un sitio web a fin de activar el mecanismo en el que el usuario acaba de registrarse. Para lo mismo, en la página principal de digiD el usuario ya tiene acceso directo al sitio web de activación[67] Esto previene que el

[67] Véase: https://www.digid.nl/

usuario deba navegar por todos los apartados del sitio web o en su defecto tener que recurrir al navegador o a apartados de preguntar frecuentes para encontrar el sitio web deseado.

De acuerdo con lo observamos sería conveniente y es posible:

- La reducción de la extensión de los procesos de registro y obtención. Esto podría llevarse a cabo mediante la reducción de requerimientos técnicos, mediante la propuesta de soluciones automatizadas y/o cerradas o mediante la reducción de las subtareas.
- La apuesta por soluciones *end to end,* es decir, que se le ofrezca al usuario una solución completa a partir de la cual satisfacer sus necesidades a través de un único sitio web. Es decir, que este no deba valerse de recursos externos o “parches” para finalmente obtener el mecanismo que deseaba.

6 RESULTADOS

El analisis de los diferentes mecanismos de identidad digital nos permite afirmar que estos presentan un alto grado de complejidad, no solo por los requerimientos técnicos de los procesos de registro y puesta en marcha sino tambien por lo abstracto e indefinido de su ecosistema.

Con lo indefinido y abstracto del ecosistema nos referíamos a la complejidad derivada de aspectos como la existencia de múltiples mecanismos de identidad digital, la existencia de actos de identidad digital adscritos a determinados mecanismos en exclusivo, las incoherencias en cuanto al mecanismo necesario para interactuar digitalmente, incluso la discrecionalidad por parte de la Administración Pública respecto al mecanismo requerido para llevar a cabo un determinado trámite. Estas y otras generan confusión y aturden el usuario ante un mar de alternativas difusas.

Complementariamente, se ha observado que tanto la comunicación de la información como la naturaleza de los procesos de registro y puesta en marcha dificultan la obtención de los mecanismos. Podemos hablar de una deficiente comunicación y de unos procesos laberinticos, en los que identificamos desde un vocabulario altamente técnico - en el caso de la comunicación - a la existencia de múltiples subtareas - en lo que se refiere a los procesos en sí -.

Por tanto, podemos afirmar que la complejidad técnica de la identidad digital junto con elementos que complejizan los procesos, generan barreras insalvables para un ciudadano promedio.

Por ende, sí, podemos afirmar que la complejidad de la identidad digital en España influye negativamente en el uso de los servicios públicos digitales, al fin y al cabo, se trata de un elemento “cl@ve” sin el cual el usuario no tiene acceso a ese espacio digital, a ese maravillo ecosistema en el que España sobresale.

Sin duda, el arreglo de dichas deficiencias - para el desarrollo de una identidad digital accesible y conveniente - es factible. A la vista estan las múltiples alternativas observadas y analizadas en el panorama europeo. Alternativas holísticas y de fácil acceso y uso. A través de estos, el usuario se vale de un solo

mecanismo para identificarse electrónicamente y firmar digitalmente en todos los trámites online habilitados por la Administración Pública.

7 CONCLUSIÓN

De acuerdo con el análisis realizado y los resultados obtenidos confirmamos aquello que planteábamos mediante la hipótesis, y es que, el desajuste entre la oferta y demanda de servicios públicos digitales es – en parte - atribuible a la complejidad técnica de identidad digital.

Si en España se quiere mejorar el nivel de uso de los servicios públicos digitales, se tendrían que atender – entre otras - las barreras identificadas y documentadas en el capítulo «4.2 Barreras a la identidad digital» y hacer las mejoras pertinentes.

La COVID 19 ha dejado a la vista lo dejes y carencias de la Administración Pública. Esto, junto con la presente revolución digital, ha hecho evidenciar sus fallas en el ámbito de lo digital. Sería sencillo afirmar que la *performance* digital de la Administración Pública es reflejo de su cultura -profundamente burocrática - y que la situación es insalvable.

Asimismo, cierto es que actualmente se está apostando fuertemente por la modernización de la Administración Pública, prueba de ello es que constituye una de las principales palancas[68] de inversión en el Plan de Recuperación Transformación y Resiliencia. En la misma, se contemplan entre otras, acciones encaminadas a la evolución de la identidad digital en España como las propuestas a través del «Nuevo modelo de identidad digital»[69] a partir del cual se apuesta por la seguridad, la interoperabilidad y el formato en remoto.

En terminos generales, se habla de «la definición de un nuevo modelo de identidad e identificación que facilite la usabilidad de los sistemas de identificación y firma digital de la ciudadanía» (Gobierno de España, pg. 44)

Esto previo, no solo en relación con los mecanismos que existen hoy en día, sino que se propone el desarrollo de nuevos sistemas de identificación y firma sencillos.

[68] La «Modernización de las Administraciones Públicas» se erige como componente 11 de la palanca «IV. Una Administración para el siglo XXI» del Plan de Plan de Recuperación, Transformación y Resiliencia
[69] Véase: https://espanadigital.gob.es/lineas-de-actuacion/nuevo-modelo-de-identidad-digital

Cabría determinar si, la creación de ulteriores mecanismos haría mejorar la situación. En este sentido, la Administración Pública debería ir más allá de la eficacia y eficiencia formales y aportar soluciones cualitativamente superiores, relacionalmente disruptivas y con las que el usuario se familiarice rápidamente. De nada vale multiplicar el número de mecanismos, hacerlos interoperables, adecuados a los estándares de la Unión Europea o garantizar que estos sean totalmente seguros si, dado el grado de complejidad que les envuelve, el usuario no consigue obtenerlos.

La Administración Pública, con las propuestas que plantea, debe poder ofrecer una experiencia de usuario similar a la que proporciona el sector privado que es a la que el usuario está acostumbrado. Una experiencia personalizada, flexible, accesible e intuitiva. Asi se ha conseguido en múltiples sectores en los que no podemos distinguir entre la tienda online y la tienda física, entre llamar por telefono para reservar o hacerlo a través del móvil o entre ir a comer a un restaurante o pedirlo por *take away.* Esta es la experiencia que el ciudadano como usuario debería vivir, que conciba lo digital como parte indivisible de la Administración Pública.

Queda para futuras investigaciones determinar el potencial de los mecanismos y proyectos de identidad digital como palancas de aproximación entre la ciudadanía y la Administración Pública, y si, la imagen de esta mejoraría de cara al público externo.

8 REFERENCIAS

AEFI (2 de julio, 2020) *5 claves para entender la importancia de la identidad digital en España* https://www.asociacionfintech.es/aefi-voice/5-claves-para-entender-la-importancia-de-la-identidad-digital-en-espana/#:~:text=La%20Asociaci%C3%B3n%20Espa%C3%B1ola%20de%20Fintech%20e%20Insurtech%20%28AEFI%29,econom%C3%ADa%20sumergida%2C%20liberando%20casi%20un%2014%25%20del%20PIB.

Agency for Digital Government (s.f) *eID in Denmark.* https://en.digst.dk/systems/mitid/eid-in-denmark/

Agency for Digital Government (s.f) eID in Denmark. https://en.digst.dk/systems/mitid/

ANIMSA (s.f) *Identificación y Firma Electrónica. Dos conceptos distintos.* https://www.animsa.es/noticias/identificacion-y-firma-electronica-dos-conceptos-distintos/

Android Developers (s.f) *Cómo configurar las opciones para desarrolladores en el dispositivo* https://developer.android.com/studio/debug/dev-options?hl=es-419

Arenilla, M. (2021) *La administración digital: los riesgos de la desintermediación, las escisiones y las centralizaciones.* Instituto Nacional de Administración Pública.

Avaleht - ID.ee. (2022). ID.ee. https://www.id.ee/

Bernal, M.A (2022). La identificación y autentificación electrónica ante la administración de la comunidad autónoma de Aragón. *Monografías de la Revista Aragonesa de Administración Pública* (pp. 294-317)

Casarrubios, E. (2020). *Innovación tecnológica y gestión de las tecnologías de la información y las comunicaciones en la Administración General del Estado.*

Chiarelli, F. et al. (2022). State-of-play report on public administration and digital interoperability 2022. European Comission. https://doi.org/10.2799/429353

Comisión Europea et al. (2022) *eGovernment Benchmark 2022.* https://digital-strategy.ec.europa.eu/en/library/egovernment-benchmark-2022.

Comisión Europea. (2016-2022) *“Raw Data,” e-Government Benchmark.* https://administracionelectronica.gob.es/pae_Home/pae_OBSAE/Posicionamiento-Internacional/Comision_Europea_OBSAE/benchmark-egovernment.html

Digital Iceland (s.f) *Authentication system.* https://island.is/en/authentication-system

Dirección de Sistemas de Información Departamento CERES (s.f) *MANUAL SOLICITUD CERTIFICADO PERSONA FÍSICA.* Real Casa de la Moneda – Fábrica Nacional de Moneda y Timbre. https://www.cert.fnmt.es/documents/10445900/10528353/solicitud_certificado_persona_fisica.pdf

Dirección General de Policía (s.f) *Manual y descargables de DNIeRemote.* Ministerio del Interior. https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_1015&id_menu=65

Dirección General de Policía (s.f) *Que hace falta para utilizarlo*. Ministerio del Interior. https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_300&id_menu=15

Domingo, A. (2018) *Identificación electrónica y confianza en las transacciones electrónicas: la regulación jurídico-administrativa de las instituciones de acreditación de la actuación electrónica*. Tesis doctoral, Universidad de Murcia

Dutch government (s.f) *DigiD* https://www.digid.nl/

eID software. (s. f.). https://eid.belgium.be/en/contact

European Commission. (2022). *DESI - Digital Public Services 2022.*

Felguera Garrido, E. (22 de enero, 2021) *España aprueba el primer estándar mundial sobre identidad digital descentralizada en Blockchain.* Telefónica Tech. https://empresas.blogthinkbig.com/espana-aprueba-el-primer-estandar-mundial-sobre-identidad-digital-descentralizada-en-blockchain/

Gobierno de España (2021) Componente 11. Modernización de las Administraciones públicas. https://www.lamoncloa.gob.es/temas/fondos-recuperacion/Documents/05052021-Componente11.pdf

Gobierno de España (s.f) *cl@ve.* https://clave.gob.es/clave_Home/clave.html

Gobierno de España. (2021) Plan de Recuperación, Transformación y Resiliencia. https://www.lamoncloa.gob.es/temas/fondos-recuperacion/Documents/160621-Plan_Recuperacion_Transformacion_Resiliencia.pdf.

Gobierno de España. (2022) *España digital 2026.* https://espanadigital.gob.es/sites/espanadigital/files/2022-10/Espa%C3%B1a_Digital_2026.pdf

Gobierno de España. (s.f) *Nuevo modelo de identidad digital*. https://espanadigital.gob.es/lineas-de-actuacion/nuevo-modelo-de-identidad-digital

Ibercampus (13 de diciembre, 2021) *El fracaso de la identidad digital en España lastra su buena media europea en administración electrónica: 11º en digitalización y 14º en penetración https://www.ibercampus.es/el-fracaso-de-la-identidad-digital-en-espana-lastra-su-buena-media-europea-en-administracion-electronica-queda-en-11o-puesto-de-los-27-ue-en-digitalizacion-y-14o-en-penetracion.htm*

Instituto Nacional de Estadística (INE) (2022) *Uso de productos TIC por las personas de 16 a 74 años. Problemas al utilizar un sitio web o aplicación de las administraciones o servicios públicos, por motivos particulares, en los últimos*

12 meses por características socioeconómicas. https://ine.es/jaxi/Tabla.htm?tpx=55084&L=0

Instituto Nacional de Estadística (INE) (2022) *Uso de productos TIC por las personas de 16 a 74 años. Razones para no solicitar una documentación oficial o reclamación a través de un sitio web o una aplicación de las administraciones o servicios públicos, por motivos particulares, en los últimos 12 meses, teniendo la necesidad de hacerlo por características socioeconómicas y razones declaradas.* https://ine.es/jaxi/Tabla.htm?tpx=55082&L=0

Instituto Nacional de Estadística (INE) (2022) Uso de productos TIC por las personas de 16 a 74 años. Formas de contacto o interacción con las administraciones o servicios públicos a través de Internet, por motivos particulares, en los últimos 12 meses, por características socioeconómicas y tipo de acción. https://ine.es/jaxi/Tabla.htm?tpx=50109&L=0

Johnstone, R. (16 de junio, 2022) *Digital ID – what is it, why is it needed, and how are governments developing it.* Global government forum. https://www.globalgovernmentforum.com/digital-id-what-is-it-why-is-it-needed-and-how-are-governments-developing-it/

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. *Boletín Oficial del Estado, 236, de 02 de octubre de 2015 https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565*

Ley 59/2003, de 19 de diciembre, de firma electrónica. *Boletín Oficial del Estado, 304, de 20 de diciembre de 2003 https://boe.es/buscar/act.php?id=BOE-A-2003-23399*

Lucidchart (s.f) *Qué es un diagrama de flujo https://www.lucidchart.com/pages/es/que-es-un-diagrama-de-flujo*

McKinsey & Company (octubre, 2022) How COVID-19 has pushed companies over the technology tipping point—and transformed business forever

Ministerio de Educación y Formación Profesional (s.f) *Cl@vefirma>Paso a paso. https://sede.educacion.gob.es/informacion-ayuda/soluciona-tus-dudas/firma-comun/clavefirma/paso-a-paso.html*

Molano, V. M., & Cárdenas, E. R. (2021). *Problemas y desarrollo de la identidad en el mundo digital.* Revista Chilena de Derecho y Tecnología, 10(2), 251. *https://doi.org/10.5354/0719-2584.2021.59188*

Múzquiz Jiménez, I. (8 de junio, 2023) *Identificación y firma electrónica en la Ley 39/2015.* Economist&Jurist. https://www.economistjurist.es/articulos-juridicos-destacados/identificacion-y-firma-electronica-en-la-ley-392015/

Observatorio de Administración Electrónica (OBSAE) (s.f.) *DATAOBSAE - Área Atención Ciudadano y Empresa.* https://dataobsae.administracionelectronica.gob.es/cmobsae3/dashboard/Dashboard.action?selectedIndicator=CLAVESSBD002&selectedScope=A1&selectedLevel=undefined&selectedUnit=undefined&selectedTemporalScope=1&selectedTemporal=28/02/2021#CLAVESSBD002CLAVE-summary

ONTSI (2021) *Estudio sobre digitalización de la Administración*

Ortega, S. (s.f.) *Identidad, identificación y autenticación.* https://blog.sortega.com/identidad-identificacion-y-autenticacion/

Portal Administración Electrónica (PAe) (s.f) DNI Electrónico https://firmaelectronica.gob.es/Home/Ciudadanos/DNI-Electronico.html#obtencion_dni

Portal Administración Electrónica (PAe) (s.f) *Los Certificados Electrónicos. https://firmaelectronica.gob.es/Home/Ciudadanos/Certificados-Electronicos.html*

Portal Administración electrónica (PAe) (s.f) *Resumen del posicionamiento de España Gob.es.* Gobierno de España. https://administracionelectronica.gob.es/pae_Home/pae_OBSAE/Posicionamiento-Internacional/Resumen-posicionamiento-Espana.html

Prodigioso Volcán (2022) *¿Son claros los trámites digitales?* https://comunicacionclara.com/claridad-tramites-digitales/

Ramió, C. et al. (2021) *Repensando la administración pública: administración digital e innovación pública.* Instituto Nacional de Administración Pública. Disponible en: https://cpage.mpr.gob.es/producto/repensando-la-administracion-publica/.

Real Casa de la Moneda – Fábrica Nacional de Moneda y Timbre (2017) *GUIA DE REFENCIA DEL DNIE CON NFC* https://www.dnielectronico.es/PDFs/Guia_de_Referencia_DNIe_con_NFC.pdf

Real Casa de la Moneda – Fábrica Nacional de Moneda y Timbre (s.f) *Certificado Electrónico de Ciudadano. https://www.sede.fnmt.gob.es/certificados/persona-fisica*

Real Casa de la Moneda – Fábrica Nacional de Moneda y Timbre, Cuerpo Nacional de Policía (s.f) *DNIeRemote. Manual de usuario.* Ministerio del Interior. https://www.dnielectronico.es/descargas/Apps/manual_DNIeRemote.html

Real Casa de la Moneda. Fábrica Nacional de Moneda y Timbre (27 de Octubre, 2017) *GUIA DE REFENCIA DEL DNIE CON NFC*

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). «DOUE» núm. 119, de 4 de mayo de 2016 https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE. «DOUE» núm. 257, de 28 de agosto de 2014, páginas 73 a 114 https://www.boe.es/buscar/doc.php?id=DOUE-L-2014-81822

Seguridad Social (s.f.) *Sede Electrónica. Niveles de seguridad.* https://www.seg-social.es/wps/portal/wss/internet/HerramientasWeb/4c5c5105-04d1-4dfd-8af4-1e2d5c0c1ae3/dd5a7601-1cad-497e-8455-cd06781ef25a

SK - Services - Smart-ID. (s. f.). https://www.skidsolutions.eu/en/services/smart-id/

Telefónica (11 de octubre, 2021) *La nueva identidad digital europea: los "wallets" de identidad soberana* https://empresas.blogthinkbig.com/nueva-identidad-digital-europea-wallets-identidad-soberana/

9 ANEXO I: REGISTRO Y PUESTA EN MARCHA DE LAS IDENTIDADES DIGITALES

	Clave PIN				Clave permanente				Certificado digital		DNIe	
	Registro básico		Registro Avanzado		Registo básico		Registro Avanzado				Presencialmente	
	Videollamada	Carta de invitación	Presencialmente	DNIe/certificado	Videollamada	Carta de invitación	Presencialmente	DNIe/certificado	Presencialmente mediante software	DNIe	Mediante contacto	Sin contacto (NFC)
1	Buscar «cl@ve» en el navegador	Buscar «cl@ve» en el navegador	Buscar «cl@ve» en el navegador	Buscar «cl@ve» en el navegador	Buscar «cl@ve» en el navegador	Buscar «cl@ve» en el navegador	Buscar «cl@ve» en el navegador	Buscar «cl@ve» en el navegador	Buscar «certificado digital» en el navegador	Buscar «certificado digital» en el navegador	Buscar «DNIe» en el navegador	Buscar «DNIe» en el navegador
2	Entrar en sitio web cl@ve	Entrar en sitio web cl@ve	Entrar en sitio web cl@ve	Entrar en sitio web cl@ve	Entrar en sitio web cl@ve	Entrar en sitio web cl@ve	Entrar en sitio web cl@ve	Entrar en sitio web cl@ve	Entrar en el sitio web del certificado digital	Entrar en el sitio web del certificado digital	Entrar en el sitio web del DNIe	Entrar en el sitio web del DNIe
3	Entrar en apartado web cl@ve PIN	Entrar en apartado web cl@ve PIN	Entrar en apartado web cl@ve PIN	Entrar en apartado web cl@ve PIN	Entrar en apartado web cl@ve permanente	Entrar en apartado web cl@ve permanente	Entrar en apartado web cl@ve permanente	Entrar en apartado web cl@ve permanente	Entrar en el apartado de «certificado software»	Entrar en el apartado de «certificado con DNIe»	Acceder al apartado «Cómo utilizar el DNI»	Acceder al apartado «Cómo utilizar el DNI»
4	Entrar en el apartado ¿Qué es?	Entrar en el apartado ¿Qué es?	Entrar en el apartado ¿Qué es?	Entrar en el apartado ¿Qué es?	Entrar en el apartado ¿Qué es?	Entrar en el apartado ¿Qué es?	Entrar en el apartado ¿Qué es?	Entrar en el apartado ¿Qué es?	Acceder a «configuración previa»	Acceder a «configuración previa»	Acceder al apartado «Qué hace falta para utilizarlo»	Acceder al apartado «Qué hace falta para utilizarlo»
5	Clickar en el link de registro	Clickar en el link de registro	Clickar en el link de registro	Clickar en el link de registro	Clickar en el link de registro	Clickar en el link de registro	Clickar en el link de registro	Clickar en el link de registro	Acceder al area de Descarga de Configurador FNMT	Acceder al «Área de Descarga de Configurador FNMT»	Clickar en la opción «Mediante contacto»	Clickar en la opción «Mediante antena sin contacto (NFC)»
6	Clicar la opción de registro a través de videollamada	Clicar la opción de registro a través de carta de invitación	Clicar la opción de registro a través una oficina de registro	Clicar la opción de registro a través de certificado digital o DNIe	Clicar la opción de registro a través de videollamada	Clicar la opción de registro a través de carta de invitación	Clicar la opción de registro a través una oficina de registro	Clicar la opción de registro a través de certificado digital o DNIe	Identificar y seleccionar el sowtware compatible con el equipo en el que se descarga	Identificar y seleccionar el sowtware compatible con el equipo en el que se descarga	Buscar y comprar - online u offline - un lector de tarjetas que se adeque a las especificaciones técnicas requeridas	Asegurarse de disponer de un dispositivo con las especificaciones técnicas necesarias para utilizar las tecnología NFC
7	Acceder al link Registro Cl@ve	Acceder al link Registro Cl@ve	Acceder al Buscador de Oficinas	Acceder al link Registro Cl@ve	Acceder al link Registro Cl@ve	Acceder al link Registro Cl@ve	Introducir dirección para buscar oficinas cercanas	Acceder al link Registro Cl@ve	Descargar y ejecutar el software en el equipo	Descargar y ejecutar el software en el equipo	Instalar drivers del lector de tarjetas de acuerdo a las especificaciones del fabricante	Acceder al Área de descargas
8	Clickar en la opción «Registrarse en cl@ve» del sitio web de la Agencia tributaria	Clickar en la opción «Registrarse en cl@ve» del sitio web de la Agencia tributaria	Introducir dirección para buscar oficinas cercanas	Clickar en la opción «Registrarse en Cl@ve con certificado o DNI electrónico» del sitio web de la Agencia tributaria	Clickar en la opción «Registrarse en cl@ve» del sitio web de la Agencia tributaria	Clickar en la opción «Registrarse en cl@ve» del sitio web de la Agencia tributaria	Marcar tipo de oficina cl@ve	Clickar en la opción «Registrarse en Cl@ve con certificado o DNI electrónico» del sitio web de la Agencia tributaria	Acceder al apartado de «solicitud del certificado»	Acceder al Área de descarga de la web firma electrónica para descargar Autofirma	Buscar las especificaciones online	Acceder al apartado DNIeRemote
9	Introducir DNI/NIE	Introducir DNI/NIE	Marcar tipo de oficina cl@ve	Introducir DNI/NIE	Introducir DNI/NIE	Introducir DNI/NIE	Ponerse en contacto mediante los medios habilitados	Introducir DNI/NIE	Rellenar el formulario de solicitud (DNI/NIE, primer apellido, correo electrónico)	Identificar y seleccionar el sowtware compatible con el equipo en el que se descarga	Identificar los drivers a instalar	Identificar y seleccionar la versión compatible con el equipo en el que se va a efectuar la descarga
10	Introducir fecha de validez o la de expedición	Introducir fecha de validez o la de expedición	Ponerse en contacto mediante los medios habilitados	Identifícate con tu certificado o DNI electrónico válido	Introducir fecha de validez o la de expedición	Introducir fecha de validez o la de expedición	Recibir contestación con alternativas de disponibilidad	Identifícate con tu certificado o DNI electrónico	Aceptar las condiciones de expedición del certificado y enviar petición	Acceder al «Área de descargas» del sitio web del DNIe del Cuerpo Nacional de Policía	Descargar los drivers y ejecutarlos en el ordenador	Descargar versión compatible
11	Clickar en el botón continuar	Clickar en el botón continuar	Recibir contestación con alternativas de disponibilidad	Clikar en el botón aceptar para continuar	Clickar en el botón continuar	Clickar en el botón continuar	Concertar la cita previa	Clikar en el botón aceptar para continuar	Acceder al apartado de «acreditar la identidad»	Identificar y seleccionar el software compatible con el equipo en el que se descarga	Acceder al apartado de instalación de los módulos compatibles con el equipo en el que se va a realizar la instalación	Ejecutar versión descargada en el equipo
12	Clickar en la opción "También puede registrarse por videollamada"	Clickar en la opción "Si, envíenme una carta de invitación a mi domicilio fiscal"	Concertar la cita previa	Indica un número de teléfono móvil	Clickar en la opción "También puede registrarse por videollamada"	Clickar en la opción "Si, envíenme una carta de invitación a mi domicilio fiscal"	Acudir presencialmente a la oficina de registro	Indica un número de teléfono móvil	Acceder al «Localizados de oficinas»	Descargar y ejecutar el software en el equipo	Descargar los módulos criptográficos necesarios para el sistema operativo del equipo en el que se descargaran	Acudir al repositorio oficial de Google Play
13	Realizar la "Videollamada de prueba" (recomendable)	Esperar a recibir la carta de invitación (7 días laborables)	Acudir presencialmente a la Oficina de registro	Confirma el número de teléfono introduciéndolo otra vez en la casilla siguiente	Realizar la "Videollamada de prueba" (recomendable)	Esperar a recibir la carta de invitación	Proporcionar el DNI/NIE identificativo	Confirma el número de teléfono introduciéndolo otra vez en la casilla siguiente	Seleccionar el tipo de certificado que quiere obtenerse «Persona física»	Identificar y seleccionar el software de los certificados raíces del DNIe compatibles	Ejecutar en el quipo los módulos criptográficos descargados	Buscar la aplicación móvil necesaria para hacer uso del DNIe mediante NFC
14	Clickar en el botón continuar	Localizar elcódigo CSV en la carta	Proporcionar el DNI/NIE identificativo	Aporta también una dirección de correo electrónico y confírmala de nuevo	Clickar en el botón continuar	Localizar elcódigo CSV de la carla	Obtener información con los datos de registro (entre otros el código de activación)	Aporta también una dirección de correo electrónico y confírmala de nuevo	Introducir dirección para buscar oficinas cercanas	Descargar y ejecutar los certificados raíces del DNIe		Descargar la aplicación respectiva

15	Clickar en "He accedido a la videollamada de prueba y he verificado que mi dispositivo está configurado para acceder a la videoasistencia"	Acceder al sitio web «Registrarse en cl@ve» del sitio web de la Agencia tributaria	Recibir documento con la información relativa al registro asi como el Código de Activación	Marca "Se han leído y aceptado las condiciones" y pulsa "Enviar"	Clickar en "He accedido a la videollamada de prueba y he verificado que mi dispositivo está configurado para acceder a la videoasistencia"	Acceder al sitio web Registrarse en cl@ve	Buscar «Activación cl@ve permanente»	Marca "Se han leído y aceptado las condiciones" y pulsa "Enviar"	Seleccionar la oficina más cercana	Acceder al apartado de «solicitud del certificado »		En la aplicación: selección del sistema operativo del PC
16	Acceder a la videoasistencia	Introducir DNI/NIE	Buscar la aplicación en los repositorios oficiales	Obtener información con los datos de registro	Acceder a la videoasistencia	Introducir DNI/NIE	Acceder al sitio web Características de la contraseña de Clave permanente	Obtener información con los datos de registro (entre otros el código de activación)	Llamar para pedir cita previa	Identificarse con el DNIe válido		En la aplicación: selección del medio de conexión (wifi o USB)
17	Esperar en sala de espera virtual	Introducir fecha de validez o la de expedición	Descargar aplicación en el dispositivo móvil	Buscar la aplicación en los repositorios oficiales	Esperar en sala de espera virtual	Introducir fecha de validez o la de expedición	Acceder al servicio de activación del usuario	Buscar «Activación cl@ve permanente»	Ser informado sobre el modo para pedir la cita previa	Recibir correo electrónico con Código de Solicitud		Vincular ambos dispositivos capturando el QR o conectándolo directamente mediante el cable USB
18	Acceder en el momento en el que un operador esté disponible	Marcar la opción "Ya dispongo de una carta de invitación"	Introducir DNI/NIE	Descargar aplicación en el dispositivo móvil	Acceder en el momento en el que un operador esté disponible	Marcar la opción "Ya dispongo de una carta de invitación"	Rellenar formulario (DNI/NIE, correo electrónico, código de activación, pregunta de seguridad)	Acceder al sitio web Características de la contraseña de Clave permanente	Enviar el mail poniendo en evidencia el trámite que se quiere llegar a cabo	Acceder al apartado de «descarga del certificado»		
19	Buscar la aplicación en los repositorios oficiales	Introducir Código Seguro de Verificación (CSV)	Introducir fecha de validez o de la expedición	Introducir DNI/NIE	Buscar «Activación cl@ve permanente»	Introducir Código Seguro de Verificación (CSV)	Recibir SMS con el OTP	Acceder al servicio de activación del usuario	Recibir mail con indicaciones	Rellenar el formulario junto con el código de solicitud que se le ha enviado		
20	Descargar aplicación en el dispositivo móvil	Clickar en el botón continuar	Recibir Código de activación	Fecha introducir fecha de validez o de la expedición	Acceder al sitio web Características de la contraseña de Clave permanente	Clickar en el botón continuar	Introducir OTP	Rellenar formulario (DNI/NIE, correo electrónico, código de activación, pregunta de seguridad)	correo indicando el nombre, apellidos y núm. de DNIe/TIE de la persona que precisa dicha	Aceptar los términos y condiciones de uso del certificado y descargar certificado		
21	Introducir DNI/NIE	Aportar el telefono móvil y correo electrónico	Introducir número de activación	Recibir código de activación	Acceder al servicio de activación del usuario	Aportar el telefono móvil y correo electrónico	Establecer contraseña nueva	Recibir SMS con el OTP	Recibir mail con la hora y día que se le ha asignado para la cita previa			
22	Fecha introducir fecha de validez o de la expedición	Leer y aceptar las condiciones		Introducir número de activación	Rellenar formulario (DNI/NIE, correo electrónico, código de activación, pregunta de seguridad)	Leer y aceptar las condiciones		Introducir OTP	Acudir presencialmente el día de la citación			
23	Recibir código de activación	Buscar la aplicación en los repositorios oficiales			Recibir SMS con el OTP	Buscar «Activación cl@ve permanente»		Establecer contraseña nueva	Aportar documento de identificación			
24	Introducir número de activación	Descargar aplicación en el dispositivo móvil			Introducir OTP	Acceder al sitio web Características de la contraseña de Clave permanente			Acceder al apartado «Descarga del certificado»			
25		Introducir DNI/NIE			Establecer contraseña nueva	Acceder al servicio de activación del usuario			Rellenar el formulario de solicitud (DNI/NIE, primer apellido, código de solicitud)			
26		Fecha introducir fecha de validez o de la expedición				Rellenar formulario (DNI/NIE, correo electrónico, código de activación, pregunta de seguridad)			En el equipo en el que se hizo la solicitud, descargar certificado			
27		Recibir código de activación				Recibir SMS con el OTP						
28		Introducir número de activación				Introducir OTP						
29						Establecer contraseña nueva						

Fuente: Elaboración propia a partir de sitios web oficiales