

Referencia: 2024-18-INF-4472-v1
Difusión: Limitada al expediente
Fecha: 12.02.2025

Creado por: I007
Revisado por: CALIDAD
Aprobado por: TECNICO

INFORME DE CERTIFICACIÓN

Expediente # **2024-18**

TOE **MiDNI iOS versión 1.0.0 (preproducción)**

Solicitante **Q2826004J - Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda**

Referencias

[EXT-9038] Solicitud de certificación

[EXT-9354] Informe Técnico de Evaluación

Informe de Certificación del producto MiDNI iOS versión 1.0.0 (preproducción), según la solicitud de referencia [EXT-9038], de fecha 16/04/2024, evaluado por el laboratorio DEKRA Testing and Certification S.A.U., conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-9354], recibido el pasado 25/11/2024.

CONTENIDOS

RESUMEN	3
RESUMEN DEL TOE.....	3
ACTIVIDADES DE EVALUACIÓN	8
IDENTIFICACIÓN DEL TOE	9
HIPÓTESIS Y ENTORNO DE USO	9
ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS	9
FUNCIONES DE SEGURIDAD	9
PRUEBAS DEL PRODUCTO	10
CONFIGURACIÓN EVALUADA.....	10
RESULTADOS DE LA EVALUACIÓN.....	10
RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES	10
RECOMENDACIONES DEL CERTIFICADOR	11
VALIDEZ DEL CERTIFICADO	12
GLOSARIO DE TÉRMINOS.....	12
BIBLIOGRAFÍA.....	12
DECLARACIÓN DE SEGURIDAD.....	12

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto MiDNI iOS versión 1.0.0 (preproducción).

El producto es una aplicación diseñada para dispositivos iOS que se define como “un visor de datos de identidad del usuario en dispositivos móviles”.

Solicitante:	Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda.
Organismo de Certificación:	Centro Criptológico Nacional (CCN).
Laboratorio de Evaluación:	DEKRA Testing and Certification S.A.U.
Tipo de Evaluación:	LINCE - Certificación Nacional Esencial de Seguridad, versión 2.0.
Taxonomía según CCN-STIC-140:	N/A.
Fecha de término de la evaluación:	25/11/2024.
Fecha de validez recomendada¹:	28/12/2026.

Todos los componentes de garantía requeridos por el tipo de evaluación LINCE presentan el veredicto de “PASA”. Por consiguiente, el laboratorio DEKRA Testing and Certification S.A.U. asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador para la norma Certificación Nacional Esencial de Seguridad, versión 2.0.

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto MiDNI iOS versión 1.0.0 (preproducción), se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

El objetivo de la evaluación (desde ahora en adelante las siglas TOE) es MiDNI iOS v1.0.0 (preproducción), una aplicación APP que se ejecuta en un dispositivo móvil iOS. Es responsable del establecimiento de un canal seguro TLS v1.3 de comunicación entre el TOE y los servidores de datos de los ciudadanos perteneciente a la Dirección General de la Policía de España. El canal de información establecido está cifrado y autenticado en el extremo servidor, asegurando que dicha

¹ Ver sección VALIDEZ DEL CERTIFICADO

comunicación es segura. La integridad de los datos va protegida por los *token* de integridad de Apple.

El TOE MiDNI iOS v1.0.0 (preproducción) es desarrollado por la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (desde ahora en adelante las siglas FNMT) para los dispositivos iOS. El TOE proporciona la interfaz para la visualización de sus datos identificativos, que serán descargados de servicios web externos, pero no almacenará en el dispositivo dichos datos, sólo los esenciales para el correcto funcionamiento.

NOTA: Al tratarse de una aplicación en estado de preproducción, la aplicación no se encontrará disponible en ningún market de aplicaciones.

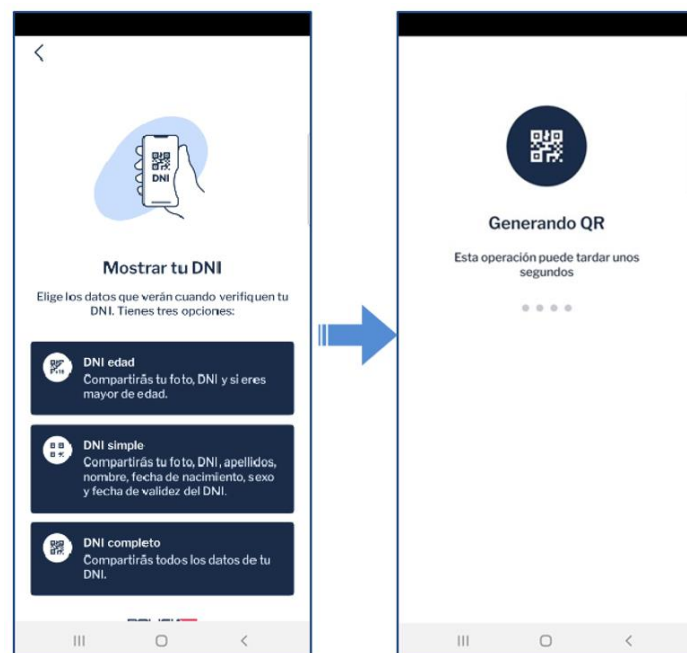


Ilustración 1: Generación de Código QR

Además, el TOE codifica y muestra en un código QR (*Quick Response*) los datos identificativos del usuario registrado y permite verificar los datos de un tercero.

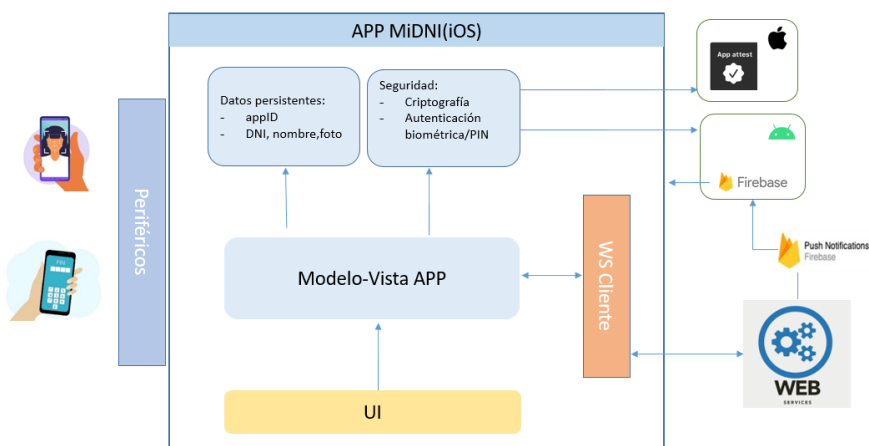


Ilustración 2: Arquitectura TOE²

La funcionalidad principal del TOE es mostrar parte de la información contenida en el Documento Nacional de Identidad (desde ahora en adelante las siglas DNI) de España en formato virtual (código QR) en vez del formato tradicional físico (tarjeta de policarbonato). Permite seleccionar entre tres únicas vistas virtuales:

- DNI EDAD: muestra la foto, número de DNI y si se es mayor de edad o no.
- DNI SIMPLE: muestra la foto, número de DNI, nombre completo, fecha nacimiento, sexo y fecha de validez.
- DNI COMPLETO: muestra el contenido completo de nuestro DNI virtual (destacar que no se incluye el número de soporte ni el equipo de expedición).

² Nótese que desde iOS también se requieren los servicios de Google para el *RemoteConfig* y las notificaciones.

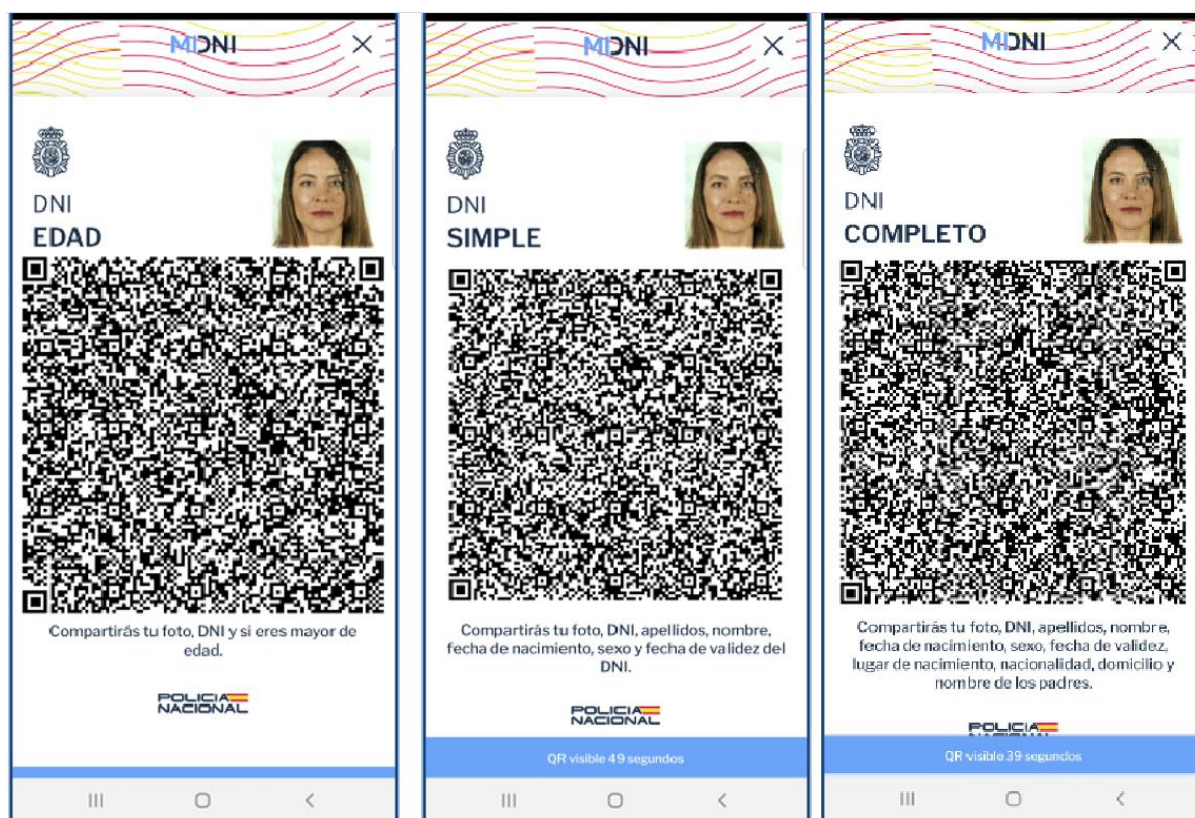


Ilustración 3: Funcionalidad principal del TOE (Generación QRs)

Estas vistas no son mostradas directamente en el dispositivo móvil iOS del usuario, sino que el TOE genera un código QR temporal que deber ser escaneado por otro usuario (en adelante el validador) usando la funcionalidad de verificación que también se proporciona en el TOE.

Nota: Cualquier usuario con el TOE puede verificar otro DNI virtual. No es necesario haberse registrado en el servicio “DNIe en el móvil” y haber virtualizado nuestro DNI para hacerlo.

Al verificar un documento, se mostrarán los datos que incluyese el código QR temporalmente generado por el titular de dicho DNI virtual:

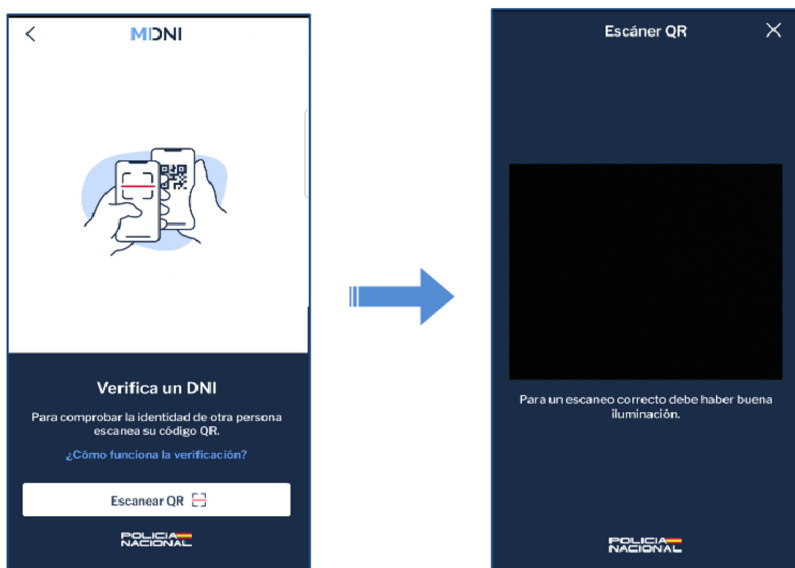


Ilustración 4: Verificación de Código QR

El TOE nos mostrará los datos del usuario incluidos en el código QR en función del tipo al que corresponde: mayor de edad, simple o completo.



Ilustración 5: Funcionalidad principal del TOE (Verificación QRs)

El código QR generado con los datos del usuario tiene un tiempo máximo de visualización. Pasado ese tiempo, la pantalla se cierra automáticamente. En esta fase de desarrollo el tiempo en pantalla es de 1 minuto.

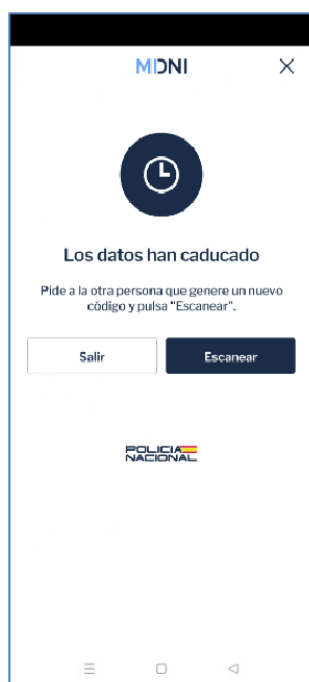


Ilustración 6: Mensaje de Caducidad de Visualización

Para realizar la funcionalidad de Virtualización o descarga de identidad (Generación de QR), se debe haber realizado previamente el registro del teléfono e identidad de una persona en una de las comisarías del Cuerpo de Policía Nacional. El registro del DNle en el Backend del Cuerpo de Policía Nacional es accesible desde:

- **Registro en la comisaría** ante un funcionario que registre el alta en el servicio.
- **Registro en PAD** de comisaría con el DNle en vigor.
- **Registro en página web** con **autenticación** con certificado DNle válido.

ACTIVIDADES DE EVALUACIÓN

El producto se evaluó con todas las evidencias necesarias para la satisfacción del tipo de evaluación LINCE, según la norma Certificación Nacional Esencial de Seguridad, versión 2.0.

Las actividades de evaluación realizadas en el transcurso de la evaluación han sido:

- ANÁLISIS DE LA DECLARACIÓN DE SEGURIDAD
- INSTALACIÓN DEL PRODUCTO
- ANÁLISIS DE CONFORMIDAD – ANÁLISIS DE LA DOCUMENTACIÓN
- ANÁLISIS DE CONFORMIDAD –PRUEBAS FUNCIONALES
- ANÁLISIS DE VULNERABILIDADES
- PRUEBAS DE PENETRACIÓN DEL TOE

IDENTIFICACIÓN DEL TOE

Objeto de evaluación (TOE): MiDNI iOS versión 1.0.0 (preproducción).

Declaración de Seguridad: MiDNI iOS Declaración de Seguridad, Versión 1.9, 21/11/2024.

HIPÓTESIS Y ENTORNO DE USO

Las hipótesis restringen las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la Declaración de Seguridad. Dichas hipótesis, se relacionan en el apartado 4.1 de la declaración de seguridad [ST].

Estas hipótesis se han aplicado durante la evaluación en la determinación de la condición de explotables de las vulnerabilidades identificadas. Por tanto, para garantizar el uso seguro del TOE, se parte de las hipótesis declaradas para su entorno de operación. En caso de que alguna de ellas no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del TOE.

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

Las amenazas detalladas en el apartado 4.3.2 de la declaración de seguridad [ST] no suponen un riesgo explotable para el producto MiDNI iOS versión 1.0.0 (preproducción), aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a moderado según lo definido en LINCE, y siempre bajo el cumplimiento de las hipótesis de uso y la correcta satisfacción de las políticas de seguridad.

Para cualquier otra amenaza no incluida en esta lista, el resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

FUNCIONES DE SEGURIDAD

El TOE declara en el apartado 5 de la declaración de seguridad [ST] las funciones de seguridad que han sido verificadas por el CCN respecto a su cumplimiento con la Taxonomía de productos declarada con respecto de la guía CCN-STIC-140 y han sido evaluadas por el laboratorio para verificar su efectividad en el entorno operacional definido.

GUÍAS DE OPERACIÓN E INSTALACIÓN DEL TOE

El producto incluye los documentos indicados a continuación, y que deberán distribuirse y facilitarse de manera conjunta a los usuarios de la versión evaluada.

- MiDNI iOS Declaración de Seguridad, Versión 1.9, 21/11/2024.
- Guía de Instalación MiDNI iOS, Versión 1.2, 08/11/2024.
- Guía operacional MiDNI iOS, Versión 1.2, 08/11/2024.

PRUEBAS DEL PRODUCTO

Para verificar la funcionalidad de seguridad declarada, el laboratorio ha desarrollado una prueba por cada una de las funciones de seguridad del producto, verificando que los resultados, así obtenidos, son consistentes con lo declarado en la Declaración de Seguridad [ST].

Adicionalmente, el laboratorio ha realizado un análisis de vulnerabilidades teniendo en cuenta las funcionalidades de seguridad declaradas en la [ST] y el nivel de resistencia a atacantes con potencial de ataque moderado tal y como se define en CCN-STIC-2002. Teniendo en cuenta las potenciales vulnerabilidades extraídas de dicho análisis, el laboratorio evaluador ha realizado pruebas de penetración para verificar la explotabilidad de las mismas en el entorno de operación declarado en [ST].

Todas las pruebas se han realizado sobre un mismo escenario de pruebas, acorde al entorno de operación, identificado en la Declaración de Seguridad [ST].

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados, y en aquellos casos en los que se presentó alguna desviación respecto de lo esperado, el evaluador ha constatado que dicha variación no supone una merma en la capacidad funcional del producto conforme a lo declarado en su Declaración de Seguridad [ST].

CONFIGURACIÓN EVALUADA

Para el funcionamiento del producto conforme a la evaluación evaluada del TOE MiDNI iOS versión 1.0.0 (preproducción) es necesario disponer de los componentes software que se indican en la sección 3.1 de la declaración de seguridad [ST].

RESULTADOS DE LA EVALUACIÓN

El producto MiDNI iOS versión 1.0.0 (preproducción) ha sido evaluado en base a la Declaración de Seguridad *MiDNI iOS Declaración de Seguridad, Versión 1.9, 21/11/2024*.

Todas las actividades de evaluación requeridas por el tipo de evaluación LINC v 2.0 presentan el veredicto de “PASA”. Por consiguiente, el laboratorio DEKRA Testing and Certification S.A.U. asigna el **VEREDICTO de “PASA”** a toda la evaluación por satisfacer todas las acciones del evaluador, definidas por la norma Certificación Nacional Esencial de Seguridad, versión 2.0 para el tipo de evaluación LINC v 2.0.

RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES

A continuación, se proporcionan las recomendaciones acerca del uso seguro del producto. Estas recomendaciones han sido recopiladas a lo largo de todo el proceso de evaluación y se detallan para que sean consideradas en la utilización del producto.

- El evaluador no ha proporcionado recomendaciones o comentarios.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto MiDNI iOS versión 1.0.0 (preproducción), se propone la resolución estimatoria de la misma.

El certificador adicionalmente recomienda a los usuarios finales del TOE que tengan en cuenta las siguientes recomendaciones:

- El presente certificado cubre la funcionalidad declarada en la [ST] del TOE en su versión especificada en la sección Identificación del TOE de este informe, concretamente:
 - o MiDNI iOS versión 1.0.0 (preproducción).

No obstante, cabe señalar que en las pantallas de la aplicación móvil la versión se identifica simplemente como “Versión 1.0.0”.

- Los usuarios finales del TOE deben comprobar que las hipótesis sobre el entorno de ejecución definidas en el apartado 4.1 de la declaración de seguridad [ST] son aceptables para el caso de uso esperado del TOE.
- El desarrollador del producto declara que el TOE es compatible con versiones de iOS 14 o superiores. No obstante, la configuración evaluada en cuanto al entorno de ejecución del TOE y cubierta por el presente certificado es la especificada en el apartado 3.1 de la declaración de seguridad [ST], esto es: dispositivo móvil iPhone Xr, con iOS 17.4.1.
- Como se especifica en el apartado 5.2 de la declaración de seguridad [ST], el código QR generado con los datos del usuario pueden ser leídos por cualquier lector de QR genérico, ya que dichos datos no están cifrados en el código QR. A este respecto, el tiempo máximo de visualización de los datos del QR especificado en el apartado 2.1 de la [ST] afecta únicamente al TOE y no a cualquier otro lector de QR, si bien únicamente a través del TOE es posible verificar la validez de los datos contenidos en dicho QR.
- En cuanto a la característica de seguridad PDC.2 especificada en el apartado 5.5 de la declaración de seguridad [ST], que hace referencia al control de integridad del TOE, cabe señalar que como se indica en el mencionado apartado no es una función de seguridad implementada por el propio TOE, sino que la delega en un componente del entorno operacional –en este caso, el servidor de datos del Cuerpo Nacional de Policía- valiéndose para ello de *App Attest* con el fin de generar un par de claves en el entorno seguro del sistema operativo sobre el que se ejecuta el TOE; posteriormente gestiona la respuesta de dicho servidor e informa al usuario en consecuencia. Este mecanismo es transparente para el usuario y se lleva a cabo cada vez que se realiza alguna acción en el TOE que requiere autenticación del usuario, pero éste no puede ejecutar a demanda un control de integridad del propio TOE.
- El laboratorio evaluador indica en el Informe Técnico de Evaluación (ETR) que, como parte del análisis de vulnerabilidades, realizó el 10/07/2024 una búsqueda de vulnerabilidades públicas potencialmente relacionadas con el TOE, determinando tras analizar todas las publicadas hasta dicha fecha que ninguna de ellas afectaba al TOE.

VALIDEZ DEL CERTIFICADO

Un certificado LINCE se emite indicando la versión específica del producto que fue evaluada. Si este producto evoluciona, sus nuevas versiones no serán certificadas por defecto. El proceso de “Assurance Continuity” o continuidad de la garantía [AC] se usa para facilitar el mantenimiento del certificado en versiones nuevas del producto. Este proceso es aplicable a la certificación LINCE.

Se recomienda revisar la validez del certificado a los veinticuatro meses desde su emisión. En todo momento el desarrollador podrá optar al proceso de renovación del certificado o re-certificación del mismo, según lo establecido en el procedimiento de certificación PO-005.

GLOSARIO DE TÉRMINOS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAFÍA

Se han utilizado las siguientes normas y documentos en la evaluación del producto:

[CCN-STIC-2001]	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0. Marzo 2022. Centro Criptológico Nacional.
[CCN-STIC-2002]	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0. Marzo 2022. Centro Criptológico Nacional.
[CCN-STIC-2003]	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0. Marzo 2022. Centro Criptológico Nacional.
[CCN-STIC-2004]	Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0. Marzo 2022. Centro Criptológico Nacional.
[ST]	MiDNI iOS Declaración de Seguridad, Versión 1.9, 21/11/2024.

DECLARACIÓN DE SEGURIDAD

Junto con este Informe de Certificación, se dispone en el Organismo de Certificación de la Declaración de Seguridad completa de la evaluación:

- MiDNI iOS Declaración de Seguridad, Versión 1.9, 21/11/2024.