Referencia: 2023-28-INF-4586-v1
Difusión: Limitada al expediente
Fecha: 16.07.2025

Creado por: CERT15
Revisado por: CALIDAD
Aprobado por: TECNICO

# INFORME DE CERTIFICACIÓN

| | |
|---|---|
| Expediente # | **2023-28** |
| TOE | **Cl@ve versión 5.8.3 (Android)** |
| Solicitante | **S2800568D - SECRETARIA GENERAL DE ADMINISTRACIÓN DIGITAL. MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL** |
| Referencias | |

[EXT-8659] 2023-08-12_2023-28_solicitud_certificacion

[EXT-9425] 2025-01-16_2023-28_ETR_v2

Informe de Certificación del producto Cl@ve versión 5.8.3 (Android), según la solicitud de referencia [EXT-8659], de fecha 12/08/2023, evaluado por el laboratorio Clover Technologies, conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-9425], recibido el pasado 16/01/2025.



https://oc.ccn.cni.es
organismo.certificacion@cni.es

**CONTENIDOS**

# RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto Cl@ve versión 5.8.3 (Android).

Cl@ve Android es una aplicación para dispositivos móviles con sistema operativo Android cuyo objetivos es proporcionar, a los ciudadanos, servicios de identificación y autenticación.

| | |
|---|---|
| **Solicitante**: | SECRETARIA GENERAL DE ADMINISTRACIÓN DIGITAL. MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL. |
| **Organismo de Certificación**: | Centro Criptológico Nacional (CCN). |
| **Laboratorio de Evaluación**: | Clover Technologies. |
| **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**: | 11/06/2025. |
| **Fecha de validez recomendada[1]:** | 17/07/2027 |

Todos los componentes de garantía requeridos por el tipo de evaluación LINCE presentan el veredicto de “PASA”. Por consiguiente, el laboratorio Clover Technologies asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador para LINCE, definidas por 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 Cl@ve versión 5.8.3 (Android), se propone la resolución estimatoria de la misma.

## *RESUMEN DEL TOE*

El producto a evaluar se trata de la aplicación Cl@ve para dispositivos móviles con sistema operativo Android, actualización de la aplicación actual Cl@ve PIN. El objetivo de este producto es ofrecer a los ciudadanos los servicios relacionados con la identificación y autenticación.

Este producto cuenta con el Proveedor de Identidad de AEAT.

Actualmente, en función de la forma y el nivel de garantía del registro, diferenciamos dos niveles:

[1] Ver sección VALIDEZ DEL CERTIFICADO

- Nivel Básico: El usuario facilita los datos de forma telemática sin necesidad de una autenticación previa mediante el uso de un certificado electrónico cualificado. De esta forma, la identificación se lleva a cabo mediante el uso de datos conocidos por el usuario y la Administración.
- Nivel avanzado: Los datos se comunican de dos formas:
    - En una oficina, de forma presencial y ante un empleado de la Administración Pública habilitado para esta tarea.
    - De forma telemática, autenticado previamente con un certificado electrónico cualificado.

Se mantienen las gestiones ofrecidas anteriormente por la aplicación "Cl@ve PIN", por ejemplo, la opción de visualizar el PIN que se ha obtenido mediante una gestión a través de un navegador web, aplicación móvil con "Cl@ve PIN" o aplicaciones de terceros. También se añaden funcionalidades relacionadas a la gestión de contraseña de "Cl@ve Permanente", por ejemplo, recuperación de código de activación, activación de contraseña, etc.

El TOE no incluye el sistema operativo ni el hardware requerido para ejecutarse. De la misma manera, se limita a la aplicación móvil de **Cl@ve versión 5.8.3**, excluyendo todos los sistemas del lado servidor.

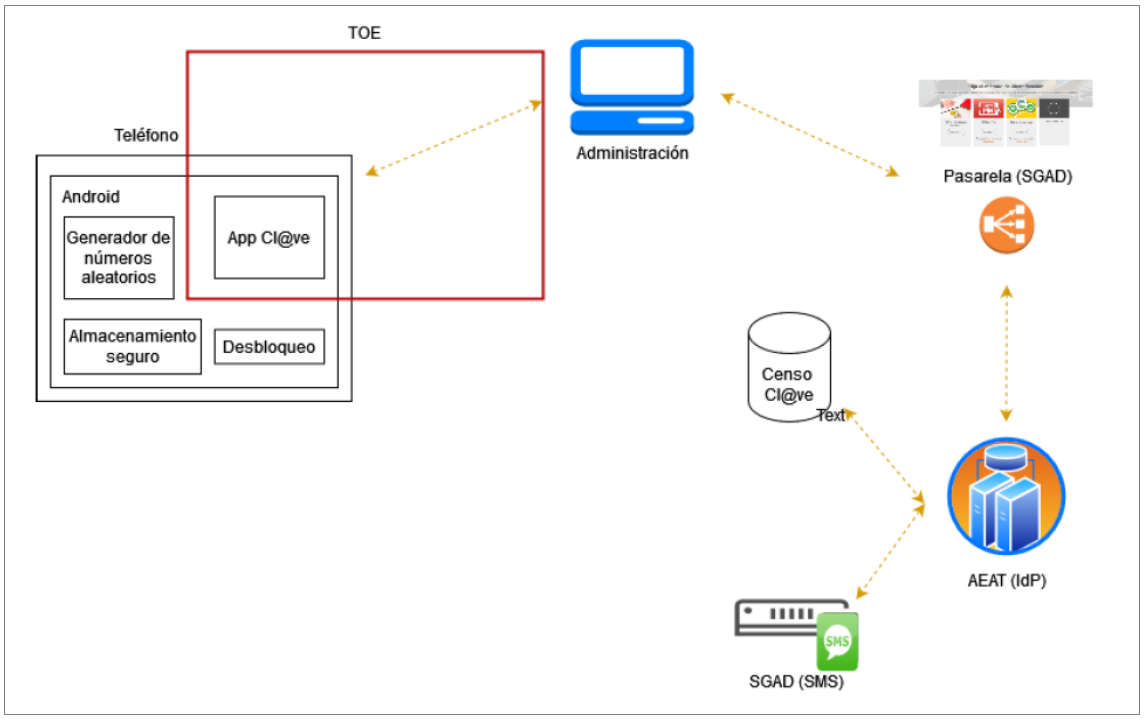


Ilustración 1 : Arquitectura y alcance del TOE.

La aplicación utiliza los siguientes recursos del sistema operativo Android:

- Generador de números aleatorios: Creación de la contraseña con la que se activa el dispositivo en el sistema Cl@ve.

- Almacenamiento seguro: Almacenamiento de las credenciales asociadas al dispositivo.
- Desbloqueo: Autenticación y autorización del usuario para utilizar la aplicación.

## *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)**: Cl@ve versión 5.8.3 (Android).

**Declaración de Seguridad:** Aplicación Cl@ve de la AEAT para Android – Declaración de Seguridad, versión 6 (08/01/2024)

## 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 *de la declaración de seguridad [ST], no suponen un riesgo explotable para* el producto Cl@ve versión 5.8.3 (Android), 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.

- Aplicación Cl@ve de la AEAT para Android – Declaración de Seguridad, versión 6 (08/01/2024)
- Guías de uso APP Cl@ve, versión 1.4 (23/10/2024).

## 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 Cl@ve versión 5.8.3 (Android) 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 Cl@ve versión 5.8.3 (Android) ha sido evaluado en base a la Declaración de Seguridad Aplicación Cl@ve de la AEAT para Android – Declaración de Seguridad, versión 6 (08/01/2024)

Todas las actividades de evaluación requeridas por el tipo de evaluación LINCE presentan el veredicto de “PASA”. Por consiguiente, el laboratorio Clover Technologies 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 LINCE.

## 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 Cl@ve versión 5.8.3 (Android), 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:
    - Cl@ve versión 5.8.3 (Android)
- 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.

## 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] Aplicación Cl@ve de la AEAT para Android – Declaración de Seguridad, versión 6 (08/01/2024)


## DECLARACIÓN DE SEGURIDAD O DECLARACIÓN DE SEGURIDAD LITE (SI APLICA)

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

- Aplicación Cl@ve de la AEAT para Android – Declaración de Seguridad, versión 6 (08/01/2024).