

Guía de Seguridad de las TIC CCN-STIC 1624

Procedimiento de empleo seguro Identity Qualification Platform (IQP) by InfoCert



Mayo de 2025





Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2025

NIPO: 083-25-206-5

Fecha de Edición: Mayo de 2025

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos

ÍNDICE

ÍNDICE.....	2
1. INTRODUCCIÓN	3
2. OBJETO Y ALCANCE	5
3. ORGANIZACIÓN DEL DOCUMENTO	7
4. FASE PREVIA A LA INSTALACIÓN.....	8
4.1 SOLICITUD Y ENTREGA SEGURA DEL SERVICIO	8
4.2 ENTORNO DE INSTALACIÓN SEGURO	8
4.3 REGISTRO Y LICENCIAS	8
4.4 CONSIDERACIONES PREVIAS.....	8
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN.....	9
5. FASE DE INSTALACIÓN.....	10
5.1 INTEGRACIÓN.....	10
6. FASE DE CONFIGURACIÓN	11
6.1 MODO DE OPERACIÓN SEGURO	11
6.2 AUTENTICACIÓN.....	11
6.3 ADMINISTRACIÓN DEL PRODUCTO.....	11
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA.....	11
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES	12
6.4 SINCRONIZACIÓN	12
6.5 ACTUALIZACIONES	12
6.6 AUDITORÍA	12
6.6.1 REGISTRO DE EVENTOS	12
6.6.2 ALMACENAMIENTO LOCAL	13
6.6.3 ALMACENAMIENTO REMOTO	13
6.7 BACKUP	13
6.8 FUNCIONES DE SEGURIDAD	13
7. FASE DE OPERACIÓN	15
8. REFERENCIAS	16
9. ABREVIATURAS.....	17

1. INTRODUCCIÓN

1. InfoCert S.p.A y CA Camerfirma S.A, como Proveedores de Servicios de Confianza Cualificados [REF1] según reglamento eIDAS tienen la capacidad, no solo de emitir certificados, sellos y sellos de tiempo cualificados, sino que también disponen de herramientas de Onboarding con módulos configurables de Identificación, de Firma Electrónica, de Comunicaciones Certificadas y de Custodia y Preservación del valor legal de los documentos.
2. Esta plataforma de herramientas configurables se denomina **TOP: Trusted Onboarding Platform** [REF2]

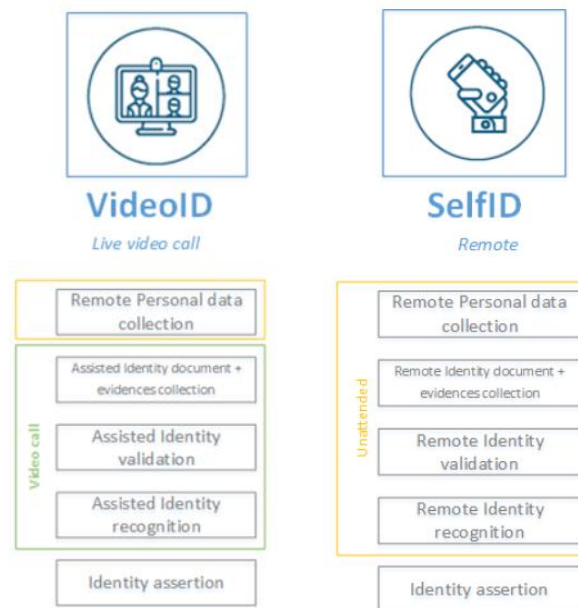


3. TOP es una Plataforma SaaS modular y multi-idioma, que incluye bloques especializados que pueden agruparse en tres categorías principales formadas por módulos independientes que pueden combinarse entre sí en función del caso de uso del cliente.
4. Los bloques, sub-bloques que forman la plataforma son:
 - Identificación:
 - Reconocimiento de Identidad: Lectura OCR, comprobación de la validez del documento de identidad.
 - Validación: implementación de controles de prueba de vida y correspondencia de caras.
 - Confirmación: revisión de los resultados del procesamiento de los puntos anteriores y confirmación de la identidad.
 - Firma Electrónica:
 - Emisión de certificados: de uso único, longevos, dominio cerrado.
 - Sistemas de autenticación de dispositivos y/o individuos: OTP SMS, OTP Push, Out of the Band.
 - Firma Electrónica, a través de aplicaciones de desarrollo propio como Gosign Desktop, Gosign web y servicios web para integrar con otras aplicaciones.
 - Otros Servicios: Composición de documentos, Comunicaciones Electrónicas Certificadas o la Custodia y Preservación del valor legal de los documentos.
5. Todos los módulos se encuentran disponibles en los siguientes idiomas: español, inglés, italiano, alemán, francés y portugués. Si fuera necesario incorporar otros idiomas, los módulos están preparados para añadir la traducción de los mensajes de manera sencilla.

6. Los servicios relacionados con la Identidad y la Validación quedan englobados dentro de la **Plataforma IQP - Identity Qualification Platform** objeto de este documento.

2. OBJETO Y ALCANCE

7. El objeto de este documento es facilitar la comprensión sobre el funcionamiento y configuración segura del proceso de Identificación desarrollado por InfoCert en su solución Identity Qualification Platform, para su solicitud y consumo por parte del cliente.
8. Para el caso que nos ocupa, se han establecido dos métodos de identificación con la configuración necesaria para operar conforme a los RFS indicados en la guía CCN-STIC 140.F11. [REF3]



9. Identity Qualification Platform se compone de los productos IQP VideoID y SelfID que han sido cualificados en CPSTIC para categoría ALTA.
 - **VideoID (asistido con operador).** Requiere de interacción entre el operador y el sujeto a identificar: el sujeto primero debe suministrar sus datos personales, selfi y documento de identidad para después iniciar una video llamada con un operador;
 - **SelfID (desasistido sin operador).** El sujeto para identificar, se toma un selfi y carga fotografías de su documento de identidad. También debe realizar una serie de gestos como prueba de vida que quedarán registrados.
10. Seguidamente, el operador encargado de la identificación deberá revisar los datos facilitados por el solicitante y analizará el resultado de las comprobaciones automáticas que la plataforma realiza sobre:
 - a) la validez y grado de autenticidad de los documentos,
 - b) grado de coincidencia entre el selfi que se ha tomado el sujeto y la fotografía en el documento de identidad,
 - c) grado de coincidencia entre la biometría facial obtenida de las fotografías y los elementos capturados como prueba de vida...etc.
11. Cada validación devuelve un valor entre 0 y 100 con el grado de cumplimiento de la validación, siendo 0 incumplimiento total y 100 el cumplimiento al completo.

12. A la vista de los resultados, el operador podrá concluir si la identificación es correcta o no.
13. Dado que la plataforma puede enviar notificaciones con el resultado de la validación a la plataforma del cliente, el cliente puede continuar con su proceso de negocio a partir de ese punto.

3. ORGANIZACIÓN DEL DOCUMENTO

14. Este documento se compone de los siguientes apartados en el que se describen las tareas y acciones a tener en cuenta durante el ciclo de vida del servicio:
- a) Apartado **4**. Fase previa a la instalación. En este apartado se describe el proceso de solicitud del servicio, características y requerimientos para llevar a cabo la integración.
 - b) Apartado **5**. Fase de instalación. En este apartado se describe la fase de integración del servicio.
 - c) Apartado **6**. Fase de configuración. En este punto se describe la configuración del servicio llevada a cabo por InfoCert, así como recomendaciones sobre la configuración del entorno del cliente.
 - d) Apartado **7**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4. FASE PREVIA A LA INSTALACIÓN

4.1 SOLICITUD Y ENTREGA SEGURA DEL SERVICIO

15. El cliente puede solicitar información para la adquisición de los servicios de la plataforma a través de la empresa del grupo InfoCert, CA Camerfirma S.A. a través de la dirección de correo comercial@camerfirma.com
16. La persona designada de Camerfirma para el proyecto se encargará de verificar el caso de uso del cliente para generar el entorno con los procesos que se ajusten a la solicitud: VideoID y/o SelfID.
17. La entrega constará de dos partes:
 - a) Información para la integración a través de servicios web para que el cliente pueda crear las peticiones de identificación desde sus aplicaciones.
 - b) Acceso a la aplicación BackOffice, IQP, para que sus operadores puedan revisar las peticiones de identificación.
18. La entrega segura de credenciales se realizará en una reunión con la persona de contacto del cliente y el jefe de proyecto designado por parte de Camerfirma e InfoCert. En esta reunión se proporcionará al cliente:
 - a) URLs de acceso al entorno Sandbox de los servicios web y plataforma IQP para realizar pruebas de integración y validación, previas a la puesta en marcha del servicio.
 - b) URL de acceso al ambiente de explotación (producción) tanto para servicios web como para la plataforma IQP.
 - c) Usuarios y contraseñas para la plataforma IQP y servicios web en todos los ambientes
 - d) Documentación de referencia para el consumo de los servicios web y de la plataforma IQP
 - e) Formación para los operadores del cliente para el manejo seguro de la plataforma IQP.

4.2 ENTORNO DE INSTALACIÓN SEGURO

19. Dado que el producto está formado por servicios web y una plataforma SaaS, IQP, no requiere de instalación por parte del cliente.

4.3 REGISTRO Y LICENCIAS

20. Los servicios prestados no requieren de licencia de instalación.
21. Se recomendará al cliente guardar de forma segura las credenciales facilitadas durante la fase de entrega segura del servicio.

4.4 CONSIDERACIONES PREVIAS

22. Es necesario que el cliente disponga de conexión a internet para consumir los servicios que se prestan a través de protocolo seguro HTTPs, TLSv1.2 o superior.
23. Los procesos de VideoID y SelfID están diseñados para que la identificación del sujeto se realice a través de dispositivos móviles.

24. Por ello, es necesario que el cliente se asegure de que los sujetos a identificar dispongan de dispositivos que:
- a) puedan recibir mensajes SMS. En el SMS se enviará un enlace para proceder a la identificación.
 - b) Dispositivos móviles con Sistema Operativo IOS 12 o superior, Android 4.1+ device (Jellybean, API Level 16).
 - c) navegador web en el dispositivo entre los que se encuentran en la lista de navegadores comprobados [REF6].
 - d) con cámara para tomar fotos de los documentos de identidad, selfis y acceder a la videollamada con operador, si procede.
 - e) Con micrófono para que en el caso de VideoID pueda interactuar con el operador durante la video llamada.
 - f) Cobertura móvil de Wi-Fi de alta velocidad y/o al menos redes 4G LTE que permitan realizar la videollamada con el operador en caso del proceso VideoID. La plataforma permite realizar una comprobación en tiempo real antes de acceder a la video llamada para asegurar que se realice con todas las garantías.
25. Los Operadores que deben verificar las peticiones de identificación y/o realizar las videollamadas deben disponer de:
- a) conexión a internet con permiso para acceder a las direcciones *.infocert.it
 - b) dispositivos cámara y micrófono para realizar la videollamada
 - c) navegador web dentro de los soportados en la lista [REF6], con permisos para acceder al micrófono y cámara del operador.
26. Si el cliente desea recibir información en tiempo real sobre el resultado de las peticiones de identificación, el Cliente deberá habilitar una URL: puerto en su organización que se configurará en la plataforma por parte del equipo de InfoCert.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

27. No se requiere de instalación de componentes de la plataforma IQP por parte del cliente en entorno de operación al ser una plataforma SaaS.

5. FASE DE INSTALACIÓN

28. El servicio no requiere instalación por parte del cliente al ser una plataforma SaaS.

5.1 INTEGRACIÓN

29. Las peticiones de video identificación se realizan a través del API de Onboarding de la plataforma **[REF5]**. Fundamentalmente, el cliente podrá implementar las siguientes operaciones:

- Crear una petición de identificación.
- Recibir información sobre el resultado de una petición de identificación.
- Recuperar las evidencias de la petición de identificación una vez completado el proceso.

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

30. El servicio que consumirá el cliente dispondrá la configuración necesaria para operar conforme a los RFS indicados en la guía CCN-STIC 140.F11 [REF3]
31. InfoCert será el encargado de mantener la configuración del producto.
32. En caso de que el cliente solicite cambios sobre los procesos, InfoCert validará que se ajusten a los RFS de la guía CCN-STIC 140.F11 [REF3] para aplicarlos en el proyecto del cliente.
33. Se configurarán los umbrales para advertir a los operadores de la puntuación obtenida en cada uno de los campos a través de un sistema de colores de la siguiente manera:

Campo	Verde	Amarillo	Rojo
Document Validity	100-90	89-70	69-0
MRZ VIZ Compliance	100-90	89-70	69-0
Anti Tampering	100-90	89-70	69-0
OCR Global	100-90	89-70	
Face Matching	100-75	N/A	74-0
Liveness	100-70	N/A	69-0

Tabla 1: Tabla de umbrales de puntuaciones

6.2 AUTENTICACIÓN

34. Existen dos (2) tipos de autenticación:
 - a) Servicios web. Autenticación básica basada, en usuario y contraseña. Todas las comunicaciones entre cliente y servidor son seguras y cifradas a través de HTTPS, TLSv1.2 o superior.
 - b) Autenticación en la plataforma IQP. El cliente acordará con el responsable de proyecto el método de autenticación de los operadores de BackOffice a acordar con el cliente entre:
 - autenticación básica usuario/contraseña: InfoCert generará los usuarios y éstos al acceder por primera vez, crearán la contraseña.
 - Integración SSO del cliente a través de protocolos OpenID Conect, SAML 2.0, OAuth 2.0, LDAP, Directorio Activo, por ejemplo. Debe ser un método de autenticación entre los compatibles con keyCloack [REF7].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

35. Los servicios de video identificación están accesibles en modo SaaS a través del protocolo seguro HTTPS, TLSv1.2 o superior.

36. La administración al módulo web BackOffice para los operadores, será administrado por InfoCert para crear y habilitar:

- Usuarios operadores y la asignación de roles.
- Configuración del servicio callback de notificaciones (opcional).

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

37. IQP soporta los siguientes perfiles de usuario:

- a) Operador: persona que accede a IQP y que realiza las verificaciones de identidad.
- b) Supervisor: persona que puede acceder a supervisar las verificaciones de varios operadores.
- c) Además, pueden asignar otros perfiles en función de la necesidad del cliente: atención al cliente, revisor... entre otros.

38. Los perfiles son gestionados directamente desde InfoCert, para tramitar la creación / borrado de usuarios deberá contactar con el soporte a través de la dirección de correo top-hd@infocert.it

39. El perfil auditor no se gestiona directamente en la plataforma, y en caso de auditorías, desde InfoCert se dará soporte al auditor para recopilar la información requerida a lo largo de los subsistemas que componen la arquitectura completa de la solución.

6.4 SINCRONIZACIÓN

40. La arquitectura de los servicios de IQP se encuentra desplegada en AWS (Amazon Web Services) y sincronizada con el servidor de tiempos AWS.

6.5 ACTUALIZACIONES

41. Las actualizaciones al ser un servicio propio se realizan de manera automática y transparente sin necesidad de parada del servicio. Se informará conveniente al cliente usuario del servicio de los cambios introducidos en cada versión.

42. Todas las actualizaciones se validan previamente en entornos previos a producción para garantizar el cumplimiento de los RFS recogidos en la guía CCN-STIC 140.F11 **[REF3]**

6.6 AUDITORÍA

6.6.1 REGISTRO DE EVENTOS

43. La gestión de los logs de la plataforma IQP está integrada en infraestructura de AWS para recopilar poder realizar diagnósticos y análisis de auditoría.

44. Los eventos que se registran son los siguientes:

- a) Login y logout de todos los usuarios.
- b) Cambio de credenciales de los usuarios administradores del servicio.
- c) Cambios en la configuración.

- d) Cualquier evento relacionado con los procesos de identificación: subida de imágenes, lectura y tratamiento de los documentos, validación de los documentos, imágenes y vídeos por parte del operador, resultados de la comparación de rostros documento-fotografías, actualización de datos realizados por el operador, momentos de inicio y fin del proceso de video identificación, actividades de rechazo de un proceso – motivos, momento -, momento de emisión y firma del informe del operador.
45. El mantenimiento de los logs se lleva cabo por jbs de acuerdo con las políticas de retención de InfoCert, conforme a la ISO 2700 en el apartado de seguridad de las operaciones. [REF8]

6.6.2 ALMACENAMIENTO LOCAL

46. Los registros de auditoría de la plataforma IQP, quedan registrados en la nube de InfoCert.
47. Se recomendará al cliente el registro de las peticiones realizadas al servicio de video identificación de cara al soporte del servicio contratado.

6.6.3 ALMACENAMIENTO REMOTO

48. La plataforma IQP almacena sus propios logs de sistema y auditoría en infraestructura Cloud.

6.7 BACKUP

49. Sobre la plataforma IQP se implementan copias de seguridad y políticas de retención de datos establecidas dentro del marco de la ISO 27001, apartado de seguridad de las operaciones. [REF8]

6.8 FUNCIONES DE SEGURIDAD

50. Los controles de seguridad establecidos en el producto aseguran el cumplimiento de los RFS indicados en la guía CCN-STIC 140.F11 [REF3]
- a) garantiza la protección frente a ataques en la captura de evidencias.
 - b) Implementa la verificación biométrica del sujeto a identificar
 - c) Implementa la validación de los documentos aportados por el sujeto a identificar
51. Además, la plataforma IQP implementa funciones de seguridad adicionales que protegen frente a los ataques descritos en el informe *“Praktischer Angriff auf Video-Ident Demonstration inhärenter Schwächen der videobasierten Echtheitsprüfung physischer ID-Dokumente”* de Martin Tschirsich- Chaos Computer Club Version 1.2, 8. August 2022. [REF9].
52. Estas protecciones adicionales son:
- a) Protección en tiempo real sobre manipulaciones del documento de identidad
 - b) Protección contra deepfakes
 - c) Protección contra la inyección de vídeo y uso de emuladores.
53. La organización podrá solicitar habilitar controles adicionales en función del caso de uso que quiera implementar, pero en ningún caso menos de las descritas en los párrafos anteriores.
54. Solo serán consideradas identificaciones completadas con éxito aquellas que hayan superado correctamente todas las comprobaciones establecidas dentro del servicio.

55. No es necesario aplicar una configuración de seguridad específica adicional a la definida en la propia organización del cliente.

7. FASE DE OPERACIÓN

56. InfoCert S.P.A será el encargado del mantenimiento y administración del servicio para asegurar que los valores asignados se mantienen y cumplen los estándares marcados dentro de la cualificación del producto.
57. InfoCert mantendrá los registros de auditoría de las peticiones de identificación creadas durante el periodo de retención acordado a la firma del contrato.
58. Se recomendará al cliente mantener un registro propio de auditoría y logs.
59. El cliente dispondrá de acceso a los canales de soporte del Grupo InfoCert y Camerfirma para el seguimiento de los tickets asociados con la operación del servicio.
60. Se recomienda a los operadores emplear los siguientes umbrales para la aceptación o rechazo de los expedientes:

Campo	Umbral
Document Validity	> 70
MRZ VIZ Compliance	> 70
Anti Tampering	> 70
OCR Global	> 70
Face Matching	> 75
Liveness	> 70

Tabla 2: Tabla de umbrales de aceptación de expedientes

61. Durante la fase de operación los usuarios del servicio no podrán modificar la configuración, para solicitar cualquier cambio deberá ponerse en contacto con top-hd@infocert.it

8. REFERENCIAS

- REF1** [eIDAS Qualified Trust Service Provider](#)
- REF2** Trusted Onboarding Platform (TOP)
[TOP - Trusted Onboarding Platform - infocert.digital](https://infocert.digital/top-trusted-onboarding-platform)
- REF3** Guía 140 – Herramientas de video identificación [CCN-STIC 140.F11](#)
- REF4** Onboarding service
<https://docs.infocert.digital/top/onboarding-service/soap/overview/>
- REF5** Documentación API Onboarding
[Onboarding Service - Infocert Developers Portal](#)
- REF6** Lista de navegadores recomendados
<https://developers.infocert.digital/top-trusted-onboarding-platform/onboarding-service/browser-compatibility/>
- REF7** KeyCloack - <https://www.keycloak.org/>
- REF8** ISO27001 – certificaciones infoCert
<https://infocert.digital/certifications/>
- REF9** Chaos Computer Club – informe
[https://www.ccc.de/system/uploads/329/original/Angriff auf Video-Ident v1.2.pdf](https://www.ccc.de/system/uploads/329/original/Angriff_auf_Video-Ident_v1.2.pdf)

9. ABREVIATURAS

API	Application Programming Interface
AWS	Amazon Web Services
CCN-STIC	Centro Criptológico Nacional - Series Técnicas de Seguridad de las Tecnologías de la Información y la Comunicación
eIDAS	Electronic Identification, Authentication and Trust Services
ENS	Esquema Nacional de Seguridad.
HTTPS	Hyper Text Transfer Protocol Secure
IOS	iPhone Operating System
IQP	Identity Qualification Platform
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
OCR	Optical Character Recognition
OTP	One Time Password
QTSP	Qualified Trusted Service Provider
RFS	Requisitos Fundamentales de Seguridad
RFS	Requisitos Funcionales de seguridad
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SMS	Short Message Service
SSO	Single Sign On
TLS	Transport Security Layer
TOP	Trust Onboarding Platform
URL	Uniform Resource Locator

