Guía de Seguridad de las TIC
CCN-STIC 1638

Procedimiento de Empleo Seguro
Signaturit VideoID by Ivnosys



Noviembre 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

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.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

-

ÍNDICE

ÍNDICE 3
1. INTRODUCCIÓN 4
2. OBJETO Y ALCANCE 4
3. ORGANIZACIÓN DEL DOCUMENTO 4
4. FASE PREVIA A LA INSTALACIÓN 6
4.1 ENTREGA SEGURA DEL PRODUCTO 6
4.2 ENTORNO DE INSTALACIÓN SEGURO 6
4.3 CONSIDERACIONES PREVIAS 6
5. FASE DE INSTALACIÓN 7
6. FASE DE CONFIGURACIÓN 8
6.1 MODO DE OPERACIÓN SEGURO 8
6.2 AUTENTICACIÓN 8
6.3 ADMINISTRACIÓN DEL PRODUCTO 10
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 10
6.3.1.1 SIGNATURIT VIDEOID API 10
6.3.1.2 SIGNATURIT VIDEOID GATEWAY 11
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 12
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 12
6.5 SINCRONIZACIÓN 13
6.6 ACTUALIZACIONES 13
6.7 AUTO-CHEQUEOS 13
6.8 ALTA DISPONIBILIDAD 13
6.9 AUDITORÍA 13
6.9.1 REGISTRO DE EVENTOS 13
6.9.2 ALMACENAMIENTO LOCAL 15
6.9.3 ALMACENAMIENTO REMOTO 15
6.10 BACKUP 15
7. FASE DE OPERACIÓN 16
8. REFERENCIAS 17
9. ABREVIATURAS 18

1. INTRODUCCIÓN

La herramienta "**Signaturit VideoID by Ivnosys**" (en adelante **VideoId**) es una solución desarrollada para realizar procesos de videoidentificación de individuos (destinatarios), para su registro (Onboarding) o para la identificación de solicitantes de certificados electrónicos, que utiliza el componente biométrico (MEB) de la herramienta "Veridas Identity Verification Service" del fabricante VERIDAS y permite proceder mediante intermediación manual de un operador si lo requiere la norma, a la validación o el rechazo de las identificaciones en función de las evidencias biométricas recabadas (imágenes, vídeos) y puntuaciones procesadas por VERIDAS.

El servicio está formado por los siguientes componentes:

- **Signaturit VideoId API**: API REST encargada de proporcionar las siguientes funcionalidades:
  - Administrativa: necesaria para la gestión de solicitudes, consulta de auditoría y configuración.
  - Aplicación: su funcionalidad es indicar la versión desplegada del producto.
  - Descargas: su funcionalidad es poder descargar las evidencias generadas en el proceso de videoidentificación.
- **Signaturit VideoId Gateway**: Aplicación web que despliega la funcionalidad necesaria para la video identificación telemática de una persona, de acuerdo con los requisitos de seguridad indicados en la Guía de Seguridad de las TIC CCN-STIC 140 – anexo A.8 – **REF1**

2. OBJETO Y ALCANCE

El objeto del presente documento es facilitar la puesta en servicio, integración y configuración segura del servicio **Signaturit VideoID versión 1.15.0** para que su funcionamiento cumpla con los estándares de calidad y seguridad.

El servicio Signaturit VideoID en su versión 1.15.0 ha sido incluido en el catálogo CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [**REF15**].

3. ORGANIZACIÓN DEL DOCUMENTO

Este documento se compone de los siguientes apartados:

a) **Apartado 4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) **Apartado 5**. En este apartado se recogen recomendaciones para tener en cuenta durante la fase de instalación del producto.

c) **Apartado 6**. En este apartado se recogen las recomendaciones para tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

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 ENTREGA SEGURA DEL PRODUCTO

Para solicitar la adquisición del servicio VideoId es necesario contactar con Signaturit - Ivnosys a través de sus representantes o los canales de comunicación oficiales de la compañía, recogidos en **REF2.**

La entrega segura de las credenciales para acceder al servicio de VideoId, que se ofrece en la nube, se realizará vía email cifrado por protocolo TLS 1.2 a los correos facilitados por la organización. El usuario recibirá un nombre de usuario, un enlace seguro de un único uso con el que definirá su contraseña y la URL de acceso al entorno. El enlace de definición de contraseña tiene una validez de 48 horas.

4.2 ENTORNO DE INSTALACIÓN SEGURO

La solución Signaturit VideoID by Ivnosys está desplegada en la infraestructura cloud de Amazon Web Services (AWS), por lo que no necesita instalarse dentro del Centro de Procesamiento de Datos (CPD).

4.3 CONSIDERACIONES PREVIAS

La comunicación con Signaturit VideoID API, desplegado en internet, se realiza a través del puerto 443, protocolo HTTPS, y se protege mediante cifrado en tránsito con protocolo TLS 1.2 o TLS 1.3.

La comunicación con Signaturit VideoID Gateway, desplegado en internet, se realiza a través del puerto 443, protocolo HTTPS, y se protege mediante cifrado en tránsito con protocolo TLS 1.2

En concreto, la herramienta utiliza canales seguros basados en TLS, configurado conforme a la guia CCN-STIC 807. Estos canales no los puede configurar la organización, son los establecidos para todas las organizaciones del producto.

Si la organización quisiera recibir callbacks con información sobre los cambios de estado de las solicitudes, se debe habilitar una URL que deberá ser comunicada a VideoId para que se configure correctamente. La organización debe informar a Signaturit - Ivnosys, a través de su representante, de la URL de la aplicación en la que desea recibir las notificaciones. Asimismo, deberá indicar el mecanismo de seguridad de la aplicación y la información necesaria para la autenticación. Un usuario con rol SysAdmin configurará los callbacks desde el área de gestión del dashboard, utilizando la información proporcionada por la organización.

Al tratarse de un servicio ofrecido en la nube, la organización que hará uso de este no deberá tener en cuenta otras consideraciones previas.

5. FASE DE INSTALACIÓN

Para la ejecución de **Signaturit VideoId by Ivnosys** no es necesaria la instalación de ningún componente o software por parte de la organización. Este es un servicio SaaS que se ofrece en la nube. Para más información, consultar el documento "*Signaturit VideoID by Ivnosys - Guía de Integración, Configuración y Operación del TOE - v. 1.15.0* – **REF4**". Este documento no es público, Signaturit - Ivnosys lo facilitará a la organización en el momento de la contratación.

Para ejecutar el módulo **Signaturit VideoID API**, se podrá usar Postman, una herramienta que permite la interacción con APIs tanto realizando peticiones, como examinando sus respuestas. Dicha herramienta se puede descargar desde la url **REF5**. Se recomienda el uso de la última versión de la aplicación, aunque se puede utilizar una versión 8 o posterior. Para conocer el proceso de instalación consultar el siguiente enlace **REF6**. Alternativamente a Postman que puede servir para pruebas de la API, el cliente puede desarrollar su propia aplicación mediante integración con Signaturit VideoID API que sería llamado directamente por dicha aplicación.

Para ejecutar **Signaturit VideoID Gateway** se deberá disponer de un dispositivo móvil con navegador web.

Relación de navegadores admitidos para la ejecución del proceso de video identificación.

Browser Name	Minimum version	Current version
Chrome	57	106
Firefox	52	105
Safari	11.2	15.6
Opera	44	90
Edge	16	103
Chrome for Android	57	103
Firefox for Android	52	101
iOS Safari	11.2	16
Opera Mobile	46	64
Samsung Internet	7.2	17

Ilustración 1. Navegadores compatibles.

Para más información, consultar el documento *"Signaturit VideoID by Ivnosys - Manual* Usuario Gateway (Configuración QTSP) - v.1.15.0. - ***REF7"***

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

El servicio de VideoId dispone de una configuración específica establecida por el mismo servicio para el cumplimiento de los RFS indicados en la guía CCN-STIC 140 – anexo A.8 – REF1. Esta configuración no puede modificarse por parte de la organización que adquiere el servicio.

Cuando se pretenda integrar el Gateway en el sitio web de la organización deberá realizarse conforme al manual de integración "Integración API Gateway Embebido 1.15.0" – **REF8** aportado por VideoId. (Documento no público)

6.2 AUTENTICACIÓN

Para el acceso a la funcionalidad de la API, se requiere la realización del proceso de inicio de sesión, mediante nombre de usuario y contraseña, que constituye el único método de autenticación posible.

Al crear un usuario este recibe un email con un enlace seguro de un único uso para definir su contraseña, esta debe respetar la siguiente complejidad:

- Tamaño mínimo de 12 caracteres.
- Tamaño máximo de 100 caracteres.
- Debe contener al menos una letra minúscula.
- Debe contener al menos una letra mayúscula.
- Debe contener al menos un número.
- Debe contener al menos un no alfanumérico.

El usuario debe agregar un número de teléfono al iniciar sesión por primera vez, se confirmará con un código OTP de 6 dígitos numéricos.

Al iniciar sesión se le pedirá un código OTP de 6 dígitos como método de segundo factor de autenticación.

Las contraseñas son almacenadas como hashes one-way de las mismas, generados mediante SHA-256 con SALT.

En caso de pérdida o bloqueo de contraseña el usuario podrá realizar la recuperación de contraseña desde formulario de login:

- Tiene que identificarse con su nombre de usuario.
- Tiene que autorizar la transacción con un código OTP enviado a su número de teléfono asociado a la cuenta.
- Recibirá un enlace seguro de un único uso para el cambio de contraseña en el correo electrónico asociado a la cuenta.
- Deberá definir una nueva contraseña con la complejidad definida.

Si el proceso de login es satisfactorio, se otorga un token, Json Web Token (JWT), firmado mediante SHA-256 con SALT, tiene una duración de 10 minutos y contiene la siguiente información del usuario codificada en el payload:

- *code*: código de usuario.
- *name*: Nombre y apellidos del usuario.
- *username*: nombre de usuario.
- *organization*: Nombre de la organización a la que pertenece el usuario.
- *organizationid*: Identificador de la organización a la que pertenece el usuario.
- *role*: rol o roles vinculados al usuario.
- *exp*: expiración del token (valor numérico JSON que representa el número de segundos desde 1970-01-01T00:00:00Z UTC hasta la fecha/hora UTC especificada, ignorando los segundos bisiestos).
- *iss*: identifica la plataforma que emitió el token.
- *aud*: identifica a los destinatarios para los que será válido el token. Si un destino no está especificado deberá rechazar la petición.

El JWT se utiliza como mecanismo de autenticación y autorización dentro de la plataforma. En primer lugar, permite identificar al usuario que ha iniciado sesión correctamente y mantener su sesión activa durante el periodo de validez del token. Adicionalmente, el JWT contiene información asociada al usuario, como sus roles o permisos, que permite determinar a qué funcionalidades o recursos puede acceder. Por tanto, para acceder a funcionalidades restringidas no basta con estar autenticado mediante un JWT válido, sino que el sistema verifica también que el usuario dispone del rol o permiso necesario.

Para el acceso a la funcionalidad de dicha API Gateway se utilizan url tokenizadas. El token utilizado en la url es exclusivo por cada solicitud y está formado por 18 caracteres alfanuméricos generados de forma aleatoria, tomando referencia el timestamp del momento de la creación de la solicitud, de esta forma se garantiza que no se puedan repetir.

Al momento de crear la solicitud, el operador debe ingresar el email del destinatario donde se enviará la URL de acceso al *onboarding*.

El token de la URL concede acceso exclusivamente al flujo de videoidentificación de la transacción concreta para la que fue generado, a través del componente Signaturit VideoID Gateway. Dicho token no permite el acceso a la API administrativa ni a ninguna otra funcionalidad del sistema.

Una vez finalizado el proceso dicho token queda inservible.

La url tokenizada para iniciar el proceso se notificará al destinatario mediante un email y dispondrá de 7 días para completar el proceso, en caso de exceder dicho plazo, el sistema automáticamente expirará la solicitud.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

La herramienta establece canales seguros cuando intercambia información sensible con entidades autorizadas o entre distintas partes del producto empleando funciones, algoritmos y protocolos que estén de acuerdo con lo establecido en la guía CCN-STIC-807 (p.ej.: HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, etc.).

En concreto, la herramienta intercambia información con los siguientes componentes externos y utiliza para ello canales seguros: TLS configurado conforme al CCN-STIC 807 - **REF9**. La organización no debe realizar ninguna configuración. Los canales de comunicación están establecidos a nivel producto para todas las organizaciones por igual.

El producto dispone de las siguientes interfaces de gestión: *Signaturit VideoID API* y *Signaturit VideoID Gateway.* En las siguientes subsecciones se muestran los requisitos de comunicación segura con los mismos.

6.3.1.1 SIGNATURIT VIDEOID API

La comunicación con Signaturit VideoID API, desplegado en internet, se realiza a través del puerto 443, protocolo HTTPS, y se protege mediante cifrado en tránsito con protocolo

TLS 1.2o 1.3. (ciphersuites no modificables al estar establecidas a nivel de código). Si los servicios externos con los que interactúa el producto no tienen activos las ciphersuites de salida detalladas a continuación, no se establecerá conexión.

Las Ciphersuites de salida (que permiten la conexión de Signaturit VideoID API con servicios externos) son las que vienen determinadas en la Guía CCN-STIC-807 y que se delimitan a nivel del software por lo que no son configurables por el cliente (la herramienta no permitirá conectar con servicios externos si no es con una Ciphersuite de la Guía), en concreto las siguientes:

- **TLSv1.2**
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- **TLSv1.3**
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256

Las Ciphersuites de entrada permitidas son las definidos por la política de seguridad de AWS: TLSv1.2_2021 que se pueden encontrar en el siguiente enlace **REF10**, en concreto las siguientes:

- **TLSv1.2**
  - ECDHE-ECDSA-AES128-GCM-SHA256
  - ECDHE-ECDSA-AES256-GCM-SHA384
  - ECDHE-ECDSA-CHACHA20-POLY1305-SHA256

- **TLSv1.3**
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256

6.3.1.2 SIGNATURIT VIDEOID GATEWAY

La comunicación con Signaturit VideoID Gateway, desplegado en internet, se realiza obligatoriamente a través del puerto 443, protocolo HTTPS, y se protege obligatoriamente mediante cifrado en tránsito con protocolo TLS 1.2 y TLS 1.3(ciphersuites no modificables al estar establecidas a nivel de código). Si los servicios externos con los que interactúa el producto no tienen activos las ciphersuites de salida detalladas a continuación, no se establecerá conexión.

Las Ciphersuites de salida (que permiten la conexión de Signaturit VideoID Gateway con servicios externos) son las que vienen determinadas en la Guía CCN-STIC-807 y que se delimitan a nivel del software por lo que no son configurables por el cliente (la herramienta no permitirá conectar con servicios externos si no es con una Ciphersuite de la Guía), en concreto las siguientes:

- **TLSv1.2**
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- **TLSv1.3**
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256

Las Ciphersuites de entrada permitidas son los definidos por la política de seguridad de AWS: TLSv1.2 y TLSv1.3 que se pueden encontrar en el siguiente enlace **REF10**, en concreto las siguientes:

- **TLSv1.2**
  - ECDHE-ECDSA-AES128-GCM-SHA256
  - ECDHE-ECDSA-AES256-GCM-SHA384
  - ECDHE-ECDSA-CHACHA20-POLY1305
- **TLSv1.3**
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

La herramienta tiene la capacidad de definir cuatro (4) tipos de roles: Operador, Administrador, Auditor y SysAdmin. Para más información consultar el manual "*Signaturit VideoId by Ivnosys – Manual Usuario Dashboard v 1.15.0* - **REF11**"

El rol SysAdmin se reserva para personal del proveedor de VideoId (Signaturit - Ivnosys), ninguna persona externa a dicha organización podrá verse asignado este rol. El usuario con rol SysAdmin podrá:

- Crear organizaciones y su configuración: tipo de organización, idioma por defecto, tiempo borrado registros auditoría.
- Crear usuarios asociados a una organización.
- Resetear contraseña de un usuario.

Los roles son acumulativos por lo tanto un usuario puede tener más de un rol asociado, siempre respetando el principio del mínimo privilegio. Estas limitaciones son:

- SysAdmin = no compatible con otros roles.
- Auditor = no compatible con otros roles.
- Operador = compatible con rol Administrador.
- Administrador = compatible con rol Operador.

Para crear un usuario, el cliente debe comunicarse con personal de Signaturit - Ivnosys para solicitar el alta de los usuarios indicando: Nombre y Apellido, Email y rol.

Un SysAdmin de la herramienta podrá acceder desde el Dashboard a la organización y crear el usuario.

El nuevo usuario recibirá las credenciales de acceso en el email indicado, estas credenciales constan de un nombre de usuario y un enlace seguro de un único uso para definir su contraseña. El enlace tiene una validez de 48 horas.

Los roles son configurados exclusivamente por un usuario con rol SysAdmin de acuerdo con la necesidad de la organización. No pueden ser configurados por un administrador local.

El producto exige una re-autenticación a los usuarios tras 30 minutos, debido a la caducidad del token. Antes de que el token expire se puede realizar una refresh del token si no, será necesario solicitar uno nuevo.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

VideoId ofrece un servicio que se encuentra alojado en la nube, por lo tanto, la organización, únicamente necesita disponer de conexión a internet a través de HTTPS.

Si la organización quisiera recibir *callbacks* con información sobre los cambios de estado de las solicitudes, deberá habilitar una URL de destino HTTPS y comunicarla a Signaturit - Ivnosys, a través de su representante, para que el rol SysAdmin la configure en el sistema. La configuración queda registrada en los logs de auditoría del sistema. Las notificaciones de *callback* se transmiten exclusivamente sobre canal seguro HTTPS con TLS conforme a la guía CCN-STIC-807; el sistema no permite configurar URLs que no empleen HTTPS. La autenticación del *callback* se realiza mediante un mecanismo de inicio de sesión previo

contra el endpoint de la organización receptora, a partir del cual se obtiene un token JWT que se incluye en la cabecera X-AUTH-TOKEN de cada notificación, garantizando así que únicamente el sistema VideoID puede enviar notificaciones válidas al receptor.

6.5 SINCRONIZACIÓN

No es necesario configurar la sincronización horaria, esta se controla desde los servicios de AWS.

6.6 ACTUALIZACIONES

Las actualizaciones del servicio por cuestiones de mejoras y de seguridad son realizadas por VideoId a través de sus *releases* mediando aviso a la organización con la debida anticipación.

6.7 AUTO-CHEQUEOS

No se realizan autochequeos de la plataforma. El servicio está monitorizado 24x7 para garantizar la disponibilidad de este.

6.8 ALTA DISPONIBILIDAD

Al tratarse de un servicio cloud, se ha configurado en AWS los recursos necesarios para asegurar la disponibilidad del producto en varias zonas de disponibilidad.

6.9 AUDITORÍA

6.9.1 REGISTRO DE EVENTOS

La herramienta genera información de auditoría al comienzo y finalización de las funciones de auditoría y cuando se produzcan ciertos eventos. Para más información al respecto, consultar el documento *"Signaturit VideoId by Ivnosys – Manual Usuario Dashboard Configuración QTSP v 1.15.0* - **REF11***"*

Los registros de auditoría contienen, al menos, la siguiente información: fecha y hora del evento, tipo de evento identificado, resultado del evento, usuario que produce el evento (si aplica).

La auditoría del proceso será accesible por el rol auditor tal y como se enseña a continuación, el acceso a estos registros es de solo lectura:

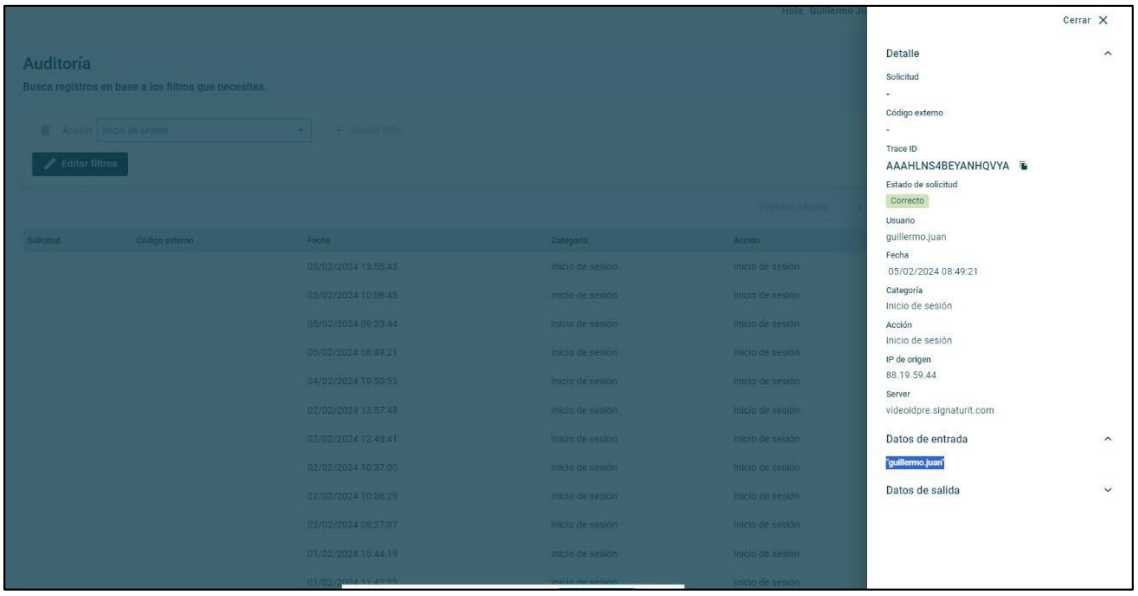


Ilustración 2. Auditoría de procesos.

La auditoría de registro de solicitudes creadas será accesible por el rol operador tal y como se enseña a continuación, este rol solo tiene permiso de lectura y está limitado a su ámbito autorizado.

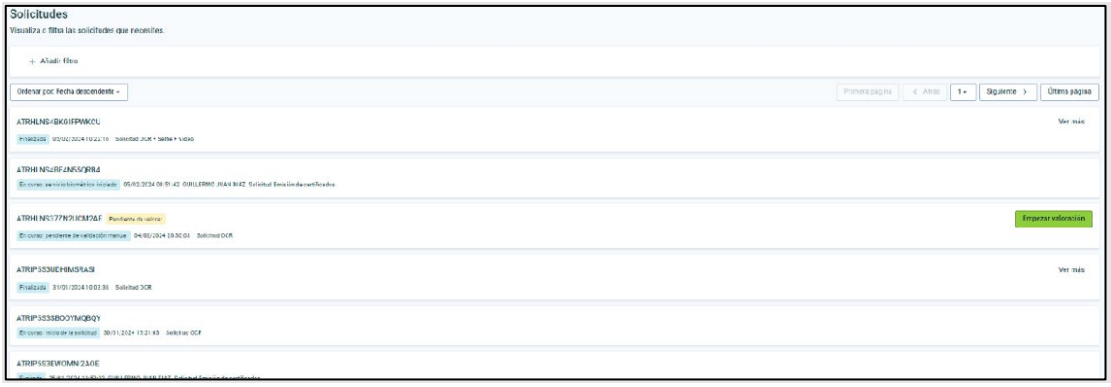


Ilustración 3. Auditoría de registros.

La herramienta registra el resultado de los procesos de verificación junto con el motivo de rechazo, en caso de tratarse de un resultado negativo.

Eliminación de los registros por organización usuaria de la herramienta: Se eliminarán de forma automática y por defecto a los 12 meses, todas las auditorías de la organización y usuarios vinculados. Este período de tiempo puede ser modificado por un usuario con rol SysAdmin si la organización contratara otro plazo de almacenamiento diferente.

Eliminación de los registros por tipo de solicitud/flujo se eliminarán en los siguientes plazos:

- A los 12 meses por defecto para flujos no QTSP. Excepto que la organización quiera un período de conservación diferente; en este caso un usuario con rol SysAdmin podrá configurarlo.
- A los 15 años + vigencia del certificado + 1 día de la finalización (Flujo QTSP finalizado y se ha emitido certificado). Este período de almacenamiento no se puede modificar, conforme a lo establecido en la **Orden ETD/465/2021, de 6 de mayo – REF12, por la que se regulan los métodos de identificación remota por**

vídeo para la expedición de certificados electrónicos cualificados.

- A los 5 años + 1 día de la finalización (Flujo QTSP finalizado, no se ha emitido certificado). Este período de almacenamiento no se puede modificar, conforme a lo establecido en la **Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza - REF13**, y la **Orden ETD/465/2021, de 6 de mayo – REF12**

6.9.2 ALMACENAMIENTO LOCAL

Al ser un servicio cloud, todos los registros de auditoría se almacenan en la nube, por lo tanto, no se debe realizar ninguna configuración al respecto. Los registros pueden ser consultados por un usuario con rol auditor mediante una llamada la API o desde el Dashboard. Se puede consultar el documento *"Signaturit VideoId by Ivnosys – Manual Usuario Dashboard Configuración QTSP v 1.15.0* - **REF11***".*

6.9.3 ALMACENAMIENTO REMOTO

Todos los registros están almacenados en remoto; en servidores externos controlados por Signaturit – Ivnosys (envío automático a AWS).

6.10 BACKUP

Toda la información que la herramienta conserva está bajo políticas de copias de seguridad de la información, para garantizar recuperar la información en caso de desastres o ataques.

En el caso de la información que reside en base de datos, se realiza una copia de seguridad diaria, con una retención de 7 días. A su vez, estas copias se almacenan en dos ubicaciones diferentes, separadas del resto de recursos de infraestructura de la herramienta.

Respecto a los documentos almacenados y gestionados por la herramienta, se encuentran replicados en una ubicación separada del entorno de ejecución del servicio. La sincronización entre el almacenamiento principal y la réplica es del orden de segundos, lo que garantiza una replicación casi instantánea.

Dado que Signaturit VideoID es una herramienta SaaS que no requiere de ninguna instalación por parte del usuario, no se requiere que la organización realice copia de seguridad alguna.

7. FASE DE OPERACIÓN

Para un correcto funcionamiento del servicio, la organización debe procurar que sus usuarios protejan y mantengan actualizadas sus credenciales conforme a la política aplicable.

VideoId se encarga del mantenimiento del servicio, de su adecuada funcionalidad y pone a disposición de la organización el siguiente medio de contacto para reportar incidencias o proponer mejoras **REF14**.

8. REFERENCIAS

REF1 Centro Criptológico Nacional – Guía de Seguridad de las TIC CCN-STIC 140 – Taxonomía de referencia para productos de seguridad TIC – Anexo A.8: Herramientas de Videoidentificación

REF2 Signaturit – Ivnosys. Canales de contacto oficiales. https://www.signaturit.com/es/contacto

REF3 Signaturit VideoID by Ivnosys - Informe Anexo G: Servicios en la nube. Guía de Seguridad de las TIC CCN-STIC 140.

REF4 Signaturit VideoID by Ivnosys - Guía de Integración, Configuración y Operación del TOE - v. 1.15.0

REF5 Postman. Herramienta de pruebas de API. https://www.postman.com

REF6 Postman. Guía de instalación y actualización. https://learning.postman.com/docs/getting-started/installation/installation-and-updates/

REF7 Signaturit VideoID by Ivnosys - Manual Usuario Gateway (Configuración QTSP) - v. 1.15.0

REF8 Signaturit VideoID by Ivnosys – Integración API Gateway Embebido v 1.15.0

REF9 Centro Criptológico Nacional – Guía de Seguridad de las TIC CCN-STIC-807. Criptología de empleo en el Esquema Nacional de Seguridad

REF10 Amazon Web Services. Supported protocols and ciphers between viewers and CloudFront. https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/secure-connections-supported-viewer-protocols-ciphers.html

REF11 Signaturit VideoId by Ivnosys – Manual Usuario Dashboard Configuración QTSP v 1.15.0

REF12 Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados https://www.boe.es/eli/es/o/2021/05/06/etd465

REF13 Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza https://www.boe.es/eli/es/l/2020/11/11/6

REF14 Signaturit – Ivnosys. Canal de comunicación de incidencias. https://servicedesk-spain-latam.namirial.com/hc/es

REF15 CPSTIC https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

9. ABREVIATURAS

API	Application Programming Interface
AWS	Amazon Web Services
BBDD	Base de Datos (Database)
CPD	Centro de Procesamiento de Datos (Data Processing Center)
ENS	Esquema Nacional de Seguridad.
HTTPS	HyperText Transfer Protocol Secure
IPSec	Internet Protocol Security
JWT	JSON Web Token
MEB	Componente Biométrico
MRZ	Machine Readable Zone
OTP	One Time Password
QTSP	Qualified Trust Service Provider
SaaS	Software as a Service
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
URL	Uniform Resource Locator
RFS	Requisitos Fundamentales de Seguridad