

Procedimiento de empleo seguro Signaturit VideoID by Ivnosys



Mayo 2024



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

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2024

NIPO: 083-24-199-5.

Fecha de Edición: mayo de 2024.



CENTRO CRIPTOLOGICO
NACIONAL

cn=CENTRO CRIPTOLOGICO
NACIONAL, 2.5.4.97=VATES-
S2800155J, ou=CENTRO
CRYPTOLOGICO NACIONAL,
o=CENTRO CRIPTOLOGICO
NACIONAL, c=ES
2024.05.31 13:23:15 +02'00'

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	4
3. ORGANIZACIÓN DEL DOCUMENTO	5
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	9
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA	9
6.3.1.1 SIGNATURIT VIDEOID API	9
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

1. La herramienta “**Signaturit Videold by Ivnosys**” (en adelante **Videold**) es una solución desarrollada para realizar procesos de video identificación 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 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, videos) y scores procesadas por VERIDAS.
2. El Servicio está formado por los siguientes componentes.
 - **Signaturit Videold API:** API REST Encargada de desplegar 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 video identificación.
 - **Signaturit Videold Gateway:** Aplicación web que despliega la funcionalidad necesaria para la video identificación telemática de un individuo de acuerdo con los requisitos de seguridad indicados en la guía Guía de Seguridad de las TIC CCN-STIC 140 F.11

2. OBJETO Y ALCANCE

3. El objeto del presente documento es facilitar la instalación y configuración segura del servicio **Signaturit VideoID versión 1.0** para que su funcionamiento cumpla con los estándares de calidad y seguridad.
4. El servicio Signaturit VideoID en su versión 1.0 ha sido cualificado en el catálogo CPSTIC para la familia “Herramientas de videoidentificación”.

3. ORGANIZACIÓN DEL DOCUMENTO

5. 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

6. Para solicitar la adquisición del servicio VideoID es necesario contactar con Signaturit - Ivnosys a través de sus representantes o los medios de comunicación oficiales de la compañía, recogidos en el siguiente enlace: <https://www.signaturit.com/es/contacto>.
7. La entrega segura de las credenciales para acceder al servicio de VideoID, que se ofrece en la nube, se realizará vía email a los correos informados por la organización. El usuario recibirá un nombre de usuario, una clave generada por el sistema y la URLs de acceso al entorno.

4.2 ENTORNO DE INSTALACIÓN SEGURO

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

4.3 CONSIDERACIONES PREVIAS

9. 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 / 1.3.
10. 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
11. En concreto la herramienta utiliza canales seguros: TLS configurado conforme al CCN-STIC 807. Estos canales no los puede configurar la organización, son los establecidos para todas las organizaciones del producto.
12. Si la organización quisiera recibir callbacks con información sobre los cambios de estado de las solicitudes se debe habilitar una URL que deberá ser indicada a VideoID para que se configure correctamente. La organización debe informar a Signaturit - Ivnosys, a través de su representante, la URL de su aplicación en la que quiere recibir las notificaciones, asimismo indicará el tipo de seguridad de la aplicación y la información necesaria para poder autenticarse de acuerdo a su seguridad. Un usuario con rol Sysadmin configurará los callbacks desde el área de gestión del dashboard utilizando la información proporcionada por la organización.
13. 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

14. 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 mayor información consultar el documento “*Signaturit VideoID by Ivnosys - Guía de Integración, Configuración y Operación del TOE - v. 1.0.4 – REF3*”. Este documento no es público, se facilitará por Signaturit-Ivnosys a la organización en el momento de la contratación.
15. Para ejecutar el módulo **Signaturit VideoID API**, se podrá usar POSTMAN, una herramienta que permite la interacción con APIs permitiendo realizar peticiones, como examinar sus respuestas. Dicha herramienta se puede descargar desde la web: <https://www.postman.com>, 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: <https://learning.postman.com/docs/getting-started/installation/installation-and-updates/>.
16. Alternativamente al POSTMAN que puede servir para pruebas de la API, el cliente puede desarrollar su propia aplicación integrando con Signaturit VideoID API que sería llamado directamente por dicha aplicación.
17. Para ejecutar **Signaturit VideoID Gateway** se deberá disponer de un dispositivo de escritorio o móvil con navegador web.
18. 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.

19. Para más información consultar el documento “*Signaturit VideoID by Ivnosys - Manual Usuario Gateway (Configuración QTSP) - v. 1.0.4 – REF2*”.

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

20. 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 F.11. Esta configuración no puede modificarse por parte de la organización que adquiere el servicio.
21. Cuando se pretenda embeber el Gateway dentro de la web de la organización se hará siguiendo el manual de integración “Integración API Gateway Embebido 1.0” aportado por Videoid. (Documento no público)

6.2 AUTENTICACIÓN

22. Para el acceso a la funcionalidad de la API, se requiere la realización del proceso de login, mediante un usuario y contraseña, que constituye el único método de autenticación posible.
23. Las contraseñas de usuario son recibidas por email en el momento de la creación del usuario, se generan de forma aleatoria con la siguiente complejidad:
 - Tamaño mínimo de 8 caracteres (Se podría ampliar a 12 caracteres o más. No obstante, este cambio se realiza desde BBDD por parte de Signaturit y aplicaría a todas las organizaciones del producto).
 - 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.
24. El usuario luego puede cambiar su contraseña, aunque la nueva debe respetar la complejidad establecida.
25. Las contraseñas son almacenadas como hashes one-way de las mismas, generados mediante SHA-256 con SALT.
26. En caso de pérdida o bloqueo de contraseña el operador deberá ponerse en contacto con el sysadmin para su restablecimiento.
27. 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 30 minutos y contiene la siguiente información del usuario:
 - *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.
28. El JWT concede acceso para que pueda acceder a las funcionalidades de acceso restringido, vinculado a uno o varios roles. Es decir, sirve para autenticar y para autorizar el acceso. Ya que según a la información que se desee acceder no es suficiente con estar autenticado, si no que se necesita pertenecer a un rol concreto.
 29. 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.
 30. Al momento de crear la solicitud, el operador debe ingresar el email del destinatario donde se enviará la URL de acceso al *onboarding*.
 31. El token de la url concede acceso a las funcionalidades de acceso restringido. Es decir, sirve para autenticar y autorizar el acceso a la totalidad de las funcionalidades de dicha API.
 32. Una vez finalizado el proceso dicho token queda inservible.
 33. 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

34. 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.).
35. En concreto la herramienta intercambia información con los siguientes componentes externos y utiliza para ello canales seguros: TLS configurado conforme al CCN-STIC 807. La organización no debe realizar ninguna configuración. Los canales de comunicación están en establecidos a nivel producto para todas las organizaciones por igual.
36. 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

37. 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 / 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.

38. 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_AES_256_CCM
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

TLSv1.3

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_AES_128_CCM_8_SHA256

39. Las Ciphersuites de entrada permitidas son los definidos por la política de seguridad de AWS: TLSv1.2_2021 que se pueden encontrar en el siguiente enlace: https://docs.aws.amazon.com/es_es/AmazonCloudFront/latest/DeveloperGuide/secure-connections-supported-viewer-protocols-ciphers.html , en concreto las siguientes:

TLSv1.2

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-CHACHA20-POLY1305

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. (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.

40. 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_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

TLSv1.3

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_AES_128_CCM_8_SHA256

41. Las Ciphersuites de entrada permitidas son los definidos por la política de seguridad de AWS: TLSv1.2_2021 que se pueden encontrar en el siguiente enlace: https://docs.aws.amazon.com/es_es/AmazonCloudFront/latest/DeveloperGuide/secure-connections-supported-viewer-protocols-ciphers.html, en concreto las siguientes:

TLSv1.2

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-CHACHA20-POLY1305

TLSv1.3

- TLS_AES_128_GCM_SHA256

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

42. La herramienta tiene la capacidad de definir cuatro (4) tipos de roles: Operador, Administrador, Auditor y SysAdmin. Para más información consultar el manual *“Signaturit Videold by Ivnosys – Manual Usuario Dashboard Configuración QTSP v 1.0.4 - REF4”*
43. El rol SysAdmin se reserva para personal del proveedor de Videold (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.
44. Los roles son acumulativos por lo tanto un usuario puede tener más de un rol asociado.
45. 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.
46. Un Sysadmin de la herramienta podrá acceder desde el Dashboard a la organización y crear el usuario.
47. El nuevo usuario recibirá las credenciales de acceso en el email indicado.
48. 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.
49. 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 sino será necesario solicitar uno nuevo.
50. La organización no podrá modificar otros parámetros de sesión por sí sola, se deberá solicitar a un Sysadmin que gestione estas modificaciones. No se pueden modificar a desde el dashboard, se hace a nivel de BBDD y aplicarían a todas las organizaciones del producto.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

51. Videold 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.
52. Si la organización quisiera recibir callbacks con información sobre los cambios de estado de las solicitudes debe habilitar una URL que deberá ser indicada a Videold para que se configure correctamente. La organización debe informar, a través de su representante en Signaturit - Ivnosys, la URL de su aplicación en la que quiere recibir las notificaciones, asimismo indicará el tipo de seguridad de la aplicación y la información necesaria para poder autenticarse de acuerdo con su seguridad. Un usuario con rol Sysadmin configurará los callbacks desde el área de gestión del dashboard utilizando la información proporcionada por la organización.

6.5 SINCRONIZACIÓN

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

6.6 ACTUALIZACIONES

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

6.7 AUTO-CHEQUEOS

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

6.8 ALTA DISPONIBILIDAD

56. 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

57. 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 Videold by Ivnosys – Manual Usuario Dashboard Configuración QTSP v 1.0.4 - REF4”*
58. 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).
59. La auditoría del proceso será accesible por el rol auditor tal y como se enseña a continuación

Solicitud	Código externo	Fecha	Categoría	Acción
		05/02/2024 13:55:45	Inicio de sesión	Inicio de sesión
		05/02/2024 10:08:45	Inicio de sesión	Inicio de sesión
		05/02/2024 09:23:44	Inicio de sesión	Inicio de sesión
		05/02/2024 08:49:21	Inicio de sesión	Inicio de sesión
		04/02/2024 19:30:53	Inicio de sesión	Inicio de sesión
		02/02/2024 13:57:48	Inicio de sesión	Inicio de sesión
		02/02/2024 12:43:41	Inicio de sesión	Inicio de sesión
		02/02/2024 10:37:00	Inicio de sesión	Inicio de sesión
		02/02/2024 10:06:29	Inicio de sesión	Inicio de sesión
		02/02/2024 08:27:07	Inicio de sesión	Inicio de sesión
		01/02/2024 15:44:19	Inicio de sesión	Inicio de sesión
		01/02/2024 15:44:19	Inicio de sesión	Inicio de sesión

Detalle
 Solicitud
 Código externo
 Trace ID
 Estado de solicitud
 Usuario
 Fecha
 Categoría
 Acción
 IP de origen
 Server
 Datos de entrada
 Datos de salida

Ilustración 2. Auditoría de procesos.

60. La auditoría de registro de solicitudes creadas será accesible por el rol operador tal y como se enseña a continuación.

ID	Estado	Fecha	Usuario
ATRHLS48K6FPWCU	Finalizado	05/02/2024 10:02:16	Solicitud OCR + Selfie + Video
ATRHLS48EANSQRB4	En curso (servicio biométrico iniciado)	05/02/2024 08:51:42	OUILLERMO JUAN DIAZ, Solicitud Emisión de certificados
ATRHLS37ZNUCMAE	Pendiente de validación	04/02/2024 29:30:03	Solicitud OCR
ATRPSS3UCHMSRAS	Finalizado	01/01/2024 10:03:30	Solicitud OCR
ATRPSS3BOOYMQBQY	En curso (inicio de la solicitud)	18/01/2024 15:21:03	Solicitud OCR
ATRPSS3EWMNZAOE	Finalizado	05/02/2024 15:43:19	Solicitud Emisión de certificados

Ilustración 3. Auditoría de registros.

61. La herramienta registra el resultado de los procesos de verificación junto con el motivo de rechazo, en caso de tratarse de un resultado negativo.
62. 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.
63. 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, es lo indicado legalmente.

- A los 5 años 1 día (Flujo QTSP finalizado, no se ha emitido certificado). Este período de almacenamiento no se puede modificar, es lo indicado legalmente.

6.9.2 ALMACENAMIENTO LOCAL

64. 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 a la API o desde el Dashboard. Se puede consultar el documento *“Signaturit Videoid by Ivnosys – Manual Usuario Dashboard Configuración QTSP v 1.0.4 (Punto 4.1) - REF4”*.

6.9.3 ALMACENAMIENTO REMOTO

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

6.10 BACKUP

66. 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.
67. 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.
68. 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 nos garantiza una replicación casi instantánea.
69. Dado que Signaturit VideoID es una herramienta SaaS que no requiere de ninguna instalación desde el lado del usuario, no se requiere que la organización realice copia de seguridad alguna.

7. FASE DE OPERACIÓN

70. Para un correcto funcionamiento del servicio la organización debe procurar que sus usuarios protejan y mantengan actualizadas sus credenciales.
71. Videold se encarga del mantenimiento del servicio, de su adecuada funcionalidad y pone a disposición de la organización alternativos medios de contacto para reportar incidencias o proponer mejoras.

8. REFERENCIAS

- REF1** Signaturit VideoID by Ivnosys -Informe Anexo G: Servicios en la nube
Guía de Seguridad de las TIC CCN-STIC 140
- REF2** [Signaturit VideoID by Ivnosys - Manual Usuario Gateway \(Configuración QTSP\) - v. 1.0.4"](#)
- REF3** Signaturit VideoID by Ivnosys - Guía de Integración, Configuración y Operación del TOE - v. 1.0.4
- REF4** [Signaturit Videoid by Ivnosys – Manual Usuario Dashboard Configuración QTSP v 1.0.4](#)

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

