Guía de Seguridad de las TIC
CCN-STIC 1004

Procedimiento de Empleo Seguro
Signicat VideoID High



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

1 INTRODUCCIÓN 3
1.1 APLICACIÓN PARA OPERADORES 3
1.2 APLICACIÓN DE AUDITORÍA Y DOCUMENTACIÓN 3
1.3 APLICACIÓN DE VIDEO IDENTIFICACIÓN 3
2 OBJETO Y ALCANCE 4
3 ORGANIZACIÓN DEL DOCUMENTO 4
4 FASE PREVIA A LA INTEGRACIÓN 5
4.1 ENTREGA SEGURA DEL PRODUCTO 5
4.2 ENTORNO DE INSTALACIÓN SEGURO 5
4.3 REGISTRO Y LICENCIAS 6
4.4 CONSIDERACIONES PREVIAS 7
5 INTEGRACIÓN 8
6 FASE DE CONFIGURACIÓN 9
6.1 MODO DE OPERACIÓN SEGURO 9
6.2 AUTENTICACIÓN 9
6.3 ADMINISTRACIÓN DEL PRODUCTO 9
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 9
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 9
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 10
6.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS 10
6.6 GESTIÓN DE CERTIFICADOS 10
6.7 SERVIDORES DE AUTENTICACIÓN 11
6.8 SINCRONIZACIÓN HORARIA 11
6.9 ACTUALIZACIONES 11
6.10 AUTO-CHEQUEOS 11
6.11 SNMP 11
6.12 ALTA DISPONIBILIDAD 11
6.13 AUDITORÍA 12
6.13.1 REGISTRO DE EVENTOS 12
6.13.2 ALMACENAMIENTO LOCAL 12
6.13.3 ALMACENAMIENTO REMOTO 12
6.14 BACKUP 13
6.15 SERVICIOS DE SEGURIDAD 13
7 FASE DE OPERACIÓN 14
8 REFERENCIAS 15
9 ABREVIATURAS 16

1 INTRODUCCIÓN

Signicat VideoID High 2024 (en adelante, ***VideoID***) es una solución de video identificación y verificación de identidad que permite la identificación remota del solicitante mediante la comparación de la información biométrica facial extraída del documento de identidad y la biometría facial de la persona que realiza el proceso.

Combina tecnologías de transmisión de vídeo con algoritmos de inteligencia artificial para garantizar la identificación biométrica del sujeto, así como la evaluación de ciertas características del documento de identidad.

El proceso de video identificación incluye la acreditación de identidad mediante la muestra de las dos caras del documento, su holograma y una prueba de vida. Adicionalmente, el sistema permite la validación de una OTP dentro de este proceso.

El servicio incluye también la plataforma de verificación manual de identidad por parte de un agente humano, quien posteriormente realiza la revisión manual de las evidencias recogidas, así como la evaluación de diferentes elementos de seguridad que apoyen la verificación. El proceso de identificación, por lo tanto, es desasistido y asíncrono.

El servicio está compuesto por tres módulos que se describen a continuación.

1.1 APLICACIÓN PARA OPERADORES

Aplicación Web cuyo usuario principal es el operador responsable de la verificación (también llamado agente), que dispone de los conocimientos necesarios para aceptar o rechazar una video identificación. Los vídeos terminados son despachados a este módulo que ofrece todas las capacidades necesarias para la identificación biométrica del usuario final, exponiendo claramente las evidencias recabadas y señalando posibles inconsistencias para revisión manual. La dictaminación final queda a disposición del prestador del servicio.

1.2 APLICACIÓN DE AUDITORÍA Y DOCUMENTACIÓN

Aplicación web que registra las transacciones de cada proceso. Es un elemento complementario a la video identificación para dejar constancia de su realización y del resultado de esta. Sirve al prestador del servicio y a la organización que adquiere el mismo. Permite:

- Acceder a los registros de auditoría y transacciones.
- Acceder al API token individual asignado.

Adicionalmente, incluye la documentación necesaria para facilitar la integración de las aplicaciones de la organización que van a hacer uso de ***VideoID*** con las librerías (SDKs) que implementan la experiencia de usuario (cliente) tanto para Web como para aplicaciones nativas (SDK JavaScript [REF10], SDK Android [REF6], SDK iOS [REF9]), así como toda la documentación al respecto del API del servicio de ***VideoID*** (Autenticación [REF8], servicio [REF5], Eventos [REF7]).

1.3 APLICACIÓN DE VIDEO IDENTIFICACIÓN

Módulo específico donde se lleva a cabo la parte automática de la video identificación, mediante la grabación guiada del proceso y la verificación de los requisitos fundamentales de seguridad indicados en la guía [REF1].

VideoID expone un API REST en el que se ofrecen servicios de configuración y de recuperación de datos. Estos servicios son usados por el prestador de servicios o expuestos a la organización que adquiere el servicio para su integración. La configuración incluye los siguientes aspectos de relevancia, tal y como se requieren en la guía [REF1]:

- Documentos admitidos para la video identificación.
- Elementos de seguridad activados para la video identificación. En cada caso la lógica puede ser positiva o negativa:
  - Prueba de vida.
  - Suplantación de identidad.
  - Detección de ataque de presentación (máscaras, deep fake).
  - Ataque de coerción.
  - Detección de sistema operativo manipulado o virtualizado.
  - Detección de holograma.
  - Confirmación de la integridad de datos.
  - Detección de superficie reflectante.
  - Detección de copia en blanco y negro.
  - Detección de anomalías en el documento.
  - Detección de documento expirado.
  - Comparación entre anverso y reverso del documento.

2 OBJETO Y ALCANCE

El objetivo del presente documento es detallar la configuración de seguridad del servicio ***VideoID*** para que su funcionamiento cumpla con los estándares de calidad y los Requisitos Fundamentales de Seguridad (RFS) de la guía [REF1].

VideoID es un servicio en la nube que se integra con las aplicaciones del cliente mediante APIs, y permite la video identificación y verificación de identidad de un sujeto a partir de la información biométrica extraída de su documento de identidad.

El servicio ***VideoID*** ha sido cualificado y, por lo tanto, está incluida en el catálogo de Productos y Servicios TIC (CPSTIC). Para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF11]

3 ORGANIZACIÓN DEL DOCUMENTO

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

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

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

4 FASE PREVIA A LA INTEGRACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Para solicitar la adquisición del servicio ***VideoID*** es necesario contactar con Signicat Spain a través del formulario indicado en la dirección web:

https://www.signicat.com/contact/contact-sales

La experiencia de usuario se ofrece a través de tres SDKs equivalentes que la organización que adquiere el servicio integra en sus respectivas aplicaciones:

- Web: Biblioteca de JavaScript, para aplicaciones que se ejecutan en un navegador web, tanto en escritorio como en plataformas móviles.
- iOS: para aplicaciones nativas de dispositivos con sistemas operativos iOS y iPadOS de Apple.
- Android: para aplicaciones nativas de dispositivos con sistemas operativos Android.

NOTA: en todos los casos, las librerías de usuario están optimizadas para su funcionamiento en teléfonos móviles

La entrega segura del servicio se realiza en una reunión con el representante de la organización que lo adquiere. En esta reunión se proporciona un documento con las credenciales de acceso a la cuenta asignada dentro de la plataforma para la organización, y que dispone de la siguiente información:

- API Token necesario para configurar y gestionar todas las llamadas al API.
- Usuario/contraseña para el acceso a Dashboard, donde se encuentra toda la documentación necesaria para la integración con las diferentes aplicaciones: Cliente JavaScript (SDK Web), SDK Android y SDK iOS.
- URLs de acceso a los diferentes entornos, tanto de pruebas de aceptación de usuario como entorno de explotación.
- API Token y URL del entorno de demo de la Autoridad de Registro, aplicación web que permite la verificación de la identidad por parte de un agente cualificado. De esta forma, la organización podrá realizar pruebas de su integración con esta solución.

4.2 ENTORNO DE INSTALACIÓN SEGURO

El entorno operacional del servicio VideoID se encuentra desplegado sobre infraestructura cloud de Google Cloud Platform (GCP), en un entorno gestionado por Signicat y segregado lógicamente para la prestación del servicio. La plataforma se apoya en servicios gestionados de GCP y en una arquitectura basada en contenedores orquestados mediante Kubernetes, donde se despliegan los distintos componentes que forman parte del servicio VideoID.

Los componentes del servicio se ejecutan dentro de redes virtuales privadas de GCP, con controles de segmentación de red, reglas de acceso restringidas y exposición limitada únicamente a los servicios necesarios para la operación. El acceso externo al servicio se realiza mediante interfaces seguras publicadas sobre HTTPS, empleando TLS 1.2 o superior, y restringiendo la comunicación a los puertos y protocolos necesarios para la prestación del servicio.

La infraestructura de VideoID está diseñada para proporcionar alta disponibilidad, escalabilidad y resiliencia operativa, mediante el uso de servicios gestionados, mecanismos de monitorización, balanceo de carga y recuperación automática de componentes. Los entornos de prueba y producción se mantienen separados, con configuraciones y credenciales independientes.

La gestión, operación y mantenimiento de la infraestructura cloud corresponde a Signicat, incluyendo la configuración segura de la plataforma, la monitorización, la aplicación de actualizaciones, la gestión de certificados, la protección perimetral y las medidas de seguridad necesarias para garantizar la prestación segura del servicio.

La organización que adquiere el servicio no debe desplegar componentes de VideoID en su propia infraestructura. Su integración se realiza mediante el consumo de las APIs y SDKs proporcionados por Signicat, siguiendo la documentación de integración aplicable y utilizando los mecanismos de autenticación y comunicación segura definidos para el servicio.

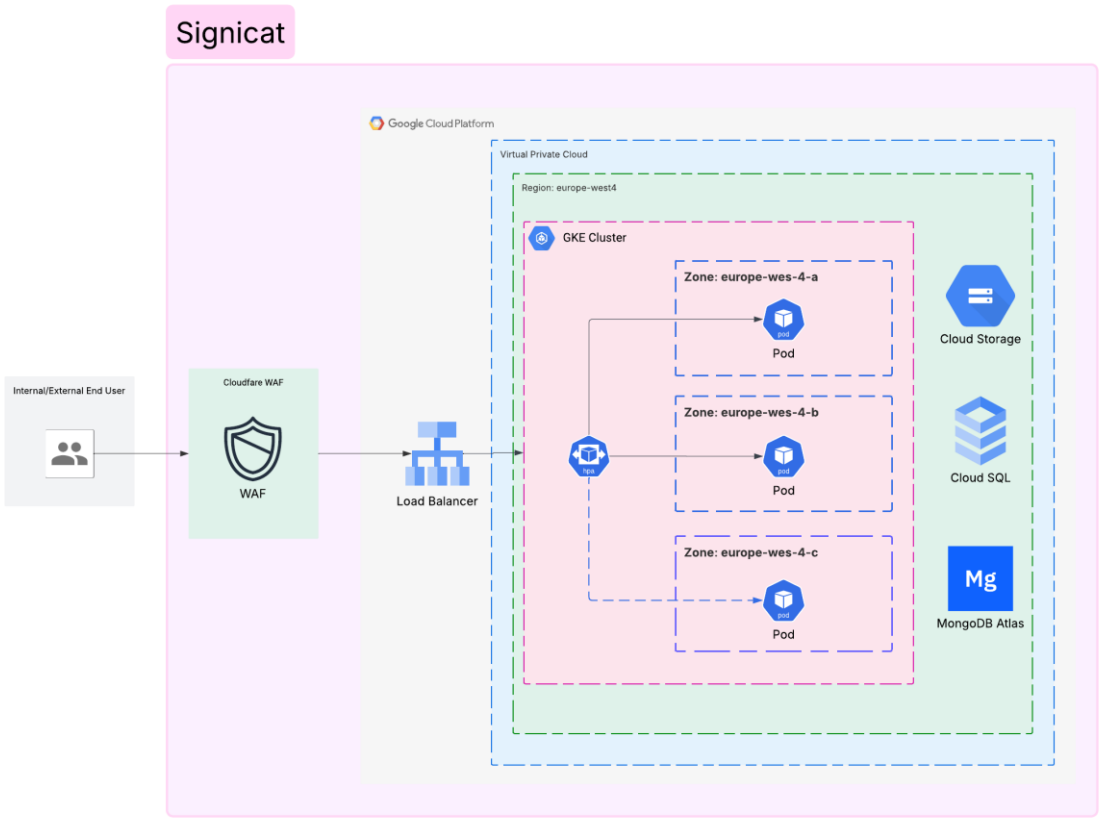


Ilustración 1. Signicat

4.3 REGISTRO Y LICENCIAS

VideoID no requiere ningún tipo de licencia más allá de lo descrito en el apartado 4.1 ENTREGA SEGURA DEL PRODUCTO.

4.4 CONSIDERACIONES PREVIAS

El servicio ***VideoID*** está accesible de forma segura a través del protocolo https con TLS 1.2 o superior, por lo que es necesario que se disponga de conexión a internet y que el puerto 443 esté abierto.

Al tratarse de un servicio ofrecido en la nube, no aplica ningún tipo de consideración previa en las infraestructuras de la organización que va a hacer uso del mismo.

5 INTEGRACIÓN

La organización que adquiere ***VideoID*** realizará la integración de su plataforma con las APIs del servicio descritas en la documentación disponible en Dashboard, bajo el menú "Documentación", en esta sección se encuentran los siguientes documentos: [REF5], [REF6], [REF7], [REF8], [REF9], [REF10].

El servicio de soporte de Signicat estará disponible para asistir en el proceso de integración a través del portal de ticketing [REF4]. Este servicio se extiende durante la duración del contrato y se encarga del seguimiento, análisis y resolución de peticiones y comentarios que puedan surgir durante el proceso de integración y servicio.

Además, en algunos casos la organización podrá contratar servicios extendidos de apoyo y mejora continua, a través de un agente dedicado de Customer Success con el que podrá comunicarse a través de su correo profesional o número de teléfono.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

El servicio ***VideoID*** deberá disponer de una configuración específica para el cumplimiento de los RFS indicados en la guía [REF1].

La descripción de la configuración estará disponible en la plataforma Dashboard, en la ruta Documentation > VideoID > Overview.

En función del SDK (Web, iOS o Android) que sea necesario integrar, se seleccionará el documento correspondiente, siempre referido a VideoID v3.

6.2 AUTENTICACIÓN

Todo integrador dispone de un Bearer Token (referido también como API Token) único para garantizar la seguridad de sus comunicaciones, proporcionado por el equipo de soporte de Signicat. El detalle de cómo usar este token y de cómo renovarlo en el caso de necesidad se detalla en el documento "api-authentication.pdf" [REF1] disponible para descarga desde la aplicación de gestión "Dashboard", en la ruta*:* "/Documentación/API Common Service/Authentication API".

Este Bearer Token permitirá la comunicación segura entre el backend desarrollado por la organización y el backend de ***VideoID.*** Entre otras funcionalidades, el uso de ese token es necesario para solicitar, cada vez que un usuario arranque el servicio, un identificador único para el proceso y un token de sesión (temporal) para ser usado desde el SDK.

Las comunicaciones entre el SDK de VideoID (integrado en la aplicación cliente) y el backend de VideoID, se realizan usando el token de sesión (único para cada transacción) y el identificador de vídeo.

Todo el proceso de solicitud de video identificación descarga de datos, descarga de vídeos, etc. se realiza de backend (organización que adquiere la solución) a backend (Signicat), empleando el Bearer Token y el identificador de vídeo único para dicha transacción.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

El módulo de Dashboard permite administrar los siguientes parámetros:

- Creación de usuarios de la organización y asignación de roles.
- Sellado de tiempo en las transacciones.
- Configuración de las URLs de Webhooks para facilitar la integración con las aplicaciones de la organización que adquiere el servicio ***VideoID***.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

El servicio ***VideoID***, mediante el módulo de Dashboard permite la definición de los siguientes roles:

- *Administrador*: Este rol dispone de los privilegios necesario para acceder a los registros de auditoría y transacciones, acceder al token de comunicación con la API,

crear usuarios y asignar roles para la plataforma Dashboard y acceder a la documentación del API.
- *Auditor*: Puede acceder a los registros de auditoría y transacciones.
- *Usuario*: Puede acceder a las transacciones.

La gestión de las contraseñas en el módulo de Dashboard responde a los siguientes requisitos:

- Debe tener una longitud mínima de 8 caracteres. En el caso de sistema ENS nivel ALTO se requiere un mínimo de 12 caracteres.
- Debe contener, al menos, una mayúscula, una minúscula, un número y un carácter especial.

Los parámetros de sesión están configurados como se indica a continuación:

- No se permiten sesiones concurrentes, pudiendo sólo existir una sesión abierta en la aplicación.
- Las sesiones se cierran pasado un tiempo de inactividad de 10 minutos.
- Se permite un máximo de 3 intentos fallidos, pasados los cuales es necesario esperar 5 minutos para volver a autenticarse.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

Al tratarse de un servicio que se ofrece en modo cloud, únicamente es necesario que la organización disponga de conexión a internet a través de https.

El puerto 443 debe estar habilitado.

6.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

El servicio VideoID, así como la comunicación entre el usuario y las interfaces de los módulos Dashboard y Autoridad de Registro, sólo funcionan con conexiones seguras vía https con TLS 1.3 en el puerto 443, por lo que deben estar disponibles desde la red de la organización.

La configuración de los protocolos soportados se realiza directamente en la infraestructura de despliegue. Se emplean los protocolos TLS 1.2 y superior.

Las suites de cifrado empleadas en la administración del servicio, así como ofrecidas por el servicio ***VideoID*** están admitidas en la guía [REF2].

TLS 1.3

```
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
```

TLS 1.2

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
```

6.6 GESTIÓN DE CERTIFICADOS

No es necesario que la organización adquirente configure ni gestione certificados digitales para el uso del servicio VideoID. La gestión del ciclo de vida de los certificados asociados a los

endpoints públicos del servicio, incluyendo su emisión, renovación y revocación, se realiza de forma gestionada por Signicat mediante Cloudflare, que proporciona mecanismos de renovación automática de certificados.

La resolución DNS del servicio se gestiona desde la infraestructura de Google Cloud Platform (GCP), y las comunicaciones externas con los endpoints del servicio se realizan mediante canales seguros HTTPS, empleando TLS 1.3 y configuraciones criptográficas alineadas con las recomendaciones de seguridad aplicables, incluyendo las indicadas en la guía CCN-STIC 807.

6.7 SERVIDORES DE AUTENTICACIÓN

No es necesario configurar servidores de autenticación en el servicio ***VideoID***.

6.8 SINCRONIZACIÓN HORARIA

No es necesario realizar ningún tipo de configuración para la sincronización horaria, ya que el servicio dispone de una sincronización horaria preconfigurada.

6.9 ACTUALIZACIONES

Al tratarse de un servicio en la nube, ***VideoID*** se actualiza de forma automática con mejoras y correcciones. Cuando estos cambios afectan sustancialmente a la funcionalidad del servicio (nuevas funcionalidades o mejoras sustanciales de funcionalidades existentes), se anuncian con anterioridad a las organizaciones usuarias del servicio.

El servicio realizará la actualización automática de firmas y motores de inspección antivirus según las recomendaciones de cada fabricante.

6.10 AUTO-CHEQUEOS

La plataforma utiliza Kubernetes como solución para la gestión automatizada de aplicaciones en contenedores. Entre sus funcionalidades, Kubernetes incluye mecanismos de auto-chequeo que supervisan continuamente el estado de los componentes desplegados (pods). En estos entornos, si un servicio presenta fallos, el sistema puede reiniciarlo automáticamente para restaurar su funcionamiento.

Además, el servicio está monitorizado 24x7 para garantizar su disponibilidad.

6.11 SNMP

No es necesaria la configuración SNMP en el servicio ***VideoID***.

6.12 ALTA DISPONIBILIDAD

Al tratarse de un servicio en la nube, ***VideoID*** se encuentra replicado en varias instancias por lo que se garantiza su disponibilidad.

6.13 AUDITORÍA

6.13.1 REGISTRO DE EVENTOS

El servicio recoge los siguientes **eventos de auditoría**, los cuales están accesibles desde distintas rutas dentro de la aplicación Dashboard, se detallan a continuación:

- Login y logout del personal autorizado, accesible desde el menú lateral izquierdo, opción "/Auditoría".
- Cambios de configuración en el servicio VideoID, accesible desde el menú lateral izquierdo, opción "/Transacciones".
- Eventos relacionados con el servicio VideoID, accesible desde el menú lateral izquierdo, opción "/Transacciones". Se registran como **transacciones**:
  - Finalización de la grabación.
  - Finalización de la consolidación y comprobación de evidencias de video y fotográficas
  - Solicitud de video identificación.
  - Aprobación de video identificación.
  - Rechazo de video identificación y sus motivos.

Así mismo, se recogen los siguientes eventos en los logs del sistema, siendo accesibles sólo por el administrador de la plataforma:

- Descripción de errores producidos.
- Accesos fallidos a la plataforma.

Para una mejor gestión de los registros de logs, la aplicación Dashboard permite su filtrado por tipo de evento.

Los eventos de auditoría disponen de los siguientes campos:

- CSV de la transacción.
- Servicio (Video en este caso).
- Tipo de evento (Solicitud verificación, Video identificación Aceptada, Video identificación Rechazada).
- Sellado de tiempo.
- Fecha y hora del evento.

6.13.2 ALMACENAMIENTO LOCAL

Todos los eventos y registros de auditoría se almacenan en la propia infraestructura cloud.

6.13.3 ALMACENAMIENTO REMOTO

Todos los eventos de auditoría se almacenan en la propia infraestructura cloud gestionada por Signicat, mediante almacenamiento compatible con el protocolo S3, dentro de los servicios habilitados para el registro, custodia y consulta de eventos asociados al servicio VideoID.

El acceso a los registros de auditoría está restringido al personal autorizado por Signicat para la administración del servicio, complementado adicionalmente con roles y permisos específicos para la operación del servicio. Estos registros se protegen frente a accesos, modificaciones o borrados no autorizados mediante los controles de acceso, segregación de funciones y mecanismos de seguridad aplicados en la infraestructura cloud del proveedor.

Los registros de auditoría se conservan de forma que permitan su trazabilidad y consulta durante los periodos definidos para el servicio. La organización adquirente puede consultar y recuperar la información de auditoría y las evidencias asociadas a sus transacciones a través de los mecanismos habilitados por la plataforma y de acuerdo con los permisos asociados al usuario autorizado.

El servicio no requiere la configuración de un sistema externo de almacenamiento remoto por parte de la organización adquirente. En caso de que la organización necesite conservar copias adicionales de los registros o evidencias en sus propios sistemas, dicha extracción deberá realizarse mediante los mecanismos de consulta, descarga o integración disponibles en la plataforma y APIs del servicio, previa autenticación mediante el API Token correspondiente, siendo responsabilidad de la organización adquirente la custodia, protección y conservación de dichas copias una vez extraídas.

Todos los eventos tienen un tamaño máximo controlado.

En cuanto al límite temporal, dependiendo del origen:

Eventos de auditoría:

i. Registro de transacciones: 15 años.

ii. Resto de eventos: durante el tiempo en el que el prestador mantiene disponible el servicio a la organización que lo adquiere.

Logs de sistema: rotación de 7 días.

6.14 BACKUP

El servicio ***VideoID*** garantiza un backup de 9 días de los datos como mínimo, realizado cada 24 horas.

6.15 SERVICIOS DE SEGURIDAD

VideoID dispone de un SOC y un WAF para garantizar la seguridad del servicio.

No es necesario aplicar ninguna configuración específica de seguridad, adicional a la definida en la propia organización.

La negociación de las claves criptográficas entre el backend de la organización y el servicio ***VideoID*** se realiza de forma automática al inicio del servicio.

7 FASE DE OPERACIÓN

Para una correcta operación del servicio, la organización deberá mantener la configuración de seguridad del producto, sin modificar los valores asignados inicialmente con la excepción de instrucciones explícitas por parte del proveedor de servicios.

La organización deberá mantener los registros de auditoría que deberán estar protegidos de borrados y modificaciones no autorizadas, y solamente el personal autorizado podrá acceder a ellos.

La información de auditoría se almacenará en las condiciones y por el periodo establecido en la normativa de seguridad.

La organización adquiriente del servicio es responsable de la recuperación y almacenaje de las evidencias necesarias para su proceso una vez concluida la identificación del sujeto, en consideración de sus requisitos operacionales, así como regulatorios y de legislación vigente.

La organización dispondrá de acceso al Centro de Soporte de Signicat (Service Desk) para el seguimiento de las incidencias (tickets) asociados con la operación del Servicio ***VideoID***.

8 REFERENCIAS

[REF1] Taxonomía de productos STIC. Anexo F.11. Herramientas de Video identificación.

[REF2] CCN-STIC 807- Criptología de empleo en el Esquema Nacional de Seguridad, Mayo 2022

[REF3] API Authentication, versión 1.2, 23/03/2023

[REF4] Eid Service Desk Internal
https://electronicid.atlassian.net/servicedesk/customer/user/login?destination=portalshttps://electronicid.atlassian.net/servicedesk/customer/user/login?destination=portals

[REF5] Service VideoID, Electronic Identification, A Signicat Company

[REF6] Android SDK VideoID 3, Electronic Identification, A Signicat Company

[REF7] Webhooks, Electronic Identification, A Signicat Company

[REF8] API Authentication, Electronic Identification, A Signicat Company

[REF9] iOS SDK VideoID 3, Electronic Identification, A Signicat Company

[REF10] JavaScript SDK ideoID 3, Electronic Identification, A Signicat Company

[REF11] *Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación del CCN.*
https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

9 ABREVIATURAS

AES	Advanced Encryption Standard
API	Application Programming Interface
CCN-STIC	Centro Criptológico Nacional Seguridad de las Tecnologías de la Información y las Comunicaciones
CPSTIC	Catálogo de Productos y Servicios TIC
CSV	Comma Separated Values
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad
GCM	Galois/Counter Mode
GCP	Google Cloud Platform
https	Hypertext Transfer Protocol Secure
iOS	iPhone Operating System
OTP	One Time Password
REST	Representational State Transfer
RFS	Requisitos Fundamentales de Seguridad
RSA	Rivest Shamir Adleman
SDK	Software Development Kit
SHA256	Secure Hash Algorithm 256
SHA384	Secure Hash Algorithm 384
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
TIC	Tecnologías de la Información y la Comunicación
TLS	Transport Layer Security
URL	Uniform Resource Locator
URLs	Uniform Resource Locators
WAF	Web Application Firewall