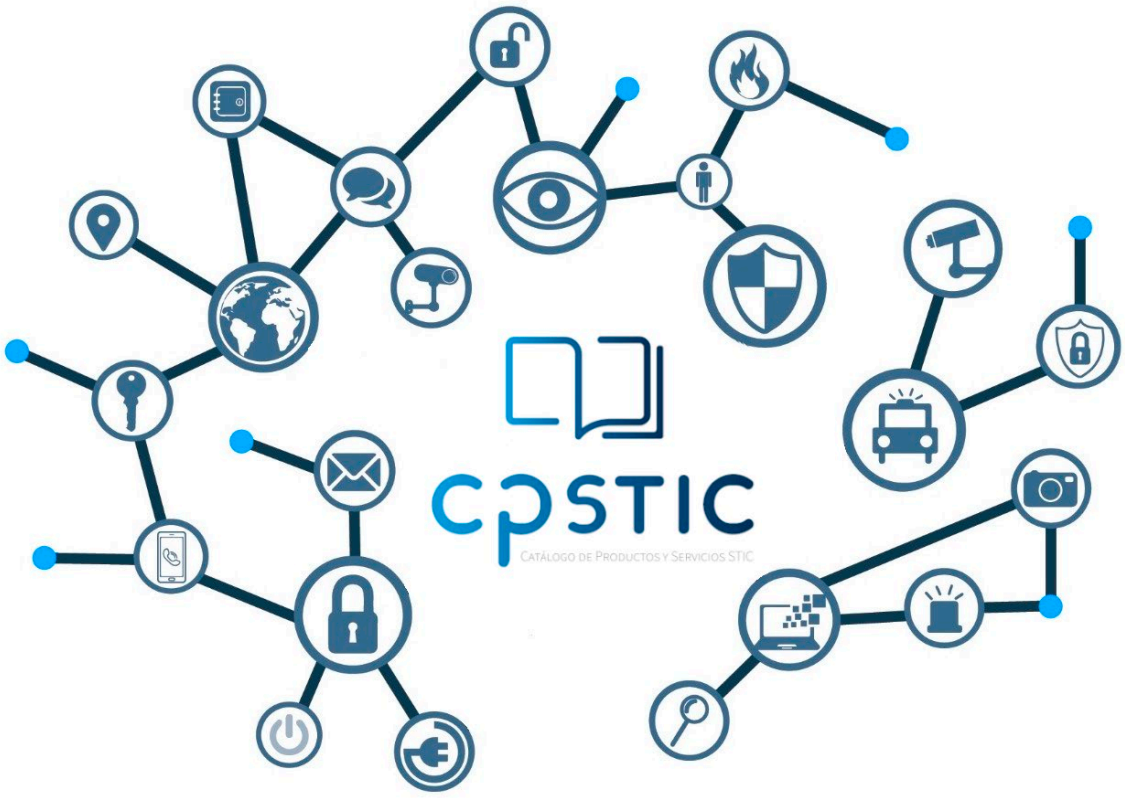
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1620

Procedimiento de Empleo Seguro
ElectronicID VideoID High Solution 3.0



Abril 2023

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

dmunguia@central.es - 7864
c=ES, o=MPR, ou=DGR,
cn=dmunguia@central.es - 7864
2023.04.03 10:11:47 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-108-9.
Fecha de Edición: abril 2023

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

ÍNDICE

1. INTRODUCCIÓN

1. ElectronicID VideoID High Solution 3.0 (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.

2. El proceso de video identificación incluye la acreditación de identidad mediante la muestra de las dos caras del documento nacional de identidad (DNI), el holograma que forma parte de dicho documento y una prueba de vida en la que se solicita al usuario que sonría. Adicionalmente, el sistema permite la validación de una OTP (*One-Time Password*) a través de SMS dentro de este proceso.

3. El servicio incluye también la plataforma de verificación de identidad por parte de un agente, donde se 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 (*unattended*) y asíncrono.

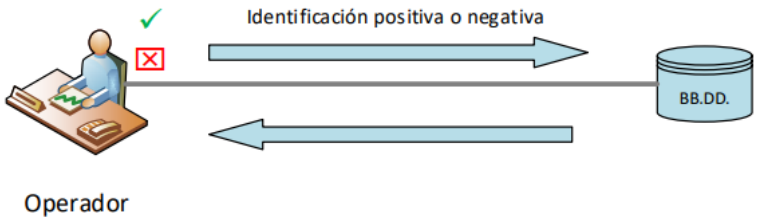


Figura 1 – Caso de uso desasistido y asíncrono

4. Con el objetivo de facilitar la comprensión del presente documento, se definen a continuación los diferentes actores que intervienen en el proceso de videoidentificación a través del servicio VideoID:

    a. **Proveedor del servicio de videodentificación:** Empresa que suministra el servicio **VideoID**, en este caso ElectronicID. El proveedor del servicio de videoidentificación es también responsable de la Autoridad de Registro (RA) como parte del mismo.

    b. **Cliente/organización que adquiere el servicio:** Empresa que integra la solución **VideoID** en su plataforma para la videoidentificación de sus clientes (usuarios finales).

    c. **Usuario final:** Sujeto que realiza el proceso de videoidentificación y cuya identidad debe ser verificada en la Autoridad de Registro de VideoID.

    d. **Agente de la Autoridad de Registro (RA):** Operador cualificado que, a través del módulo de Autoridad de Registro, realiza la verificación de la identidad mediante la visualización del vídeo y la revisión de las capturas del documento de identidad y los *checks* de seguridad resultantes del proceso de video identificación. Como resultado de esta verificación, el proceso de video identificación será aceptado o rechazado.

5. El servicio está compuesto por tres módulos:

   a. **Aplicación para Operadores:** Autoridad de Registro (*Registration Authority app - RA*)

      Aplicación Web cuyo usuario principal es el operador responsable de la verificación, 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. Su resultado queda a disposición del prestador del servicio.

   b. **Aplicación de auditoría y documentación:** *Dashboard*

      Aplicación web que permite registrar las transacciones de cada proceso de identificación. Es un elemento complementario a la video identificación para dejar constancia de su realización y del resultado de la misma. 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, que permite el acceso seguro por parte del backend del cliente a las APIs del servicio VideoID.

      Adicionalmente, incluye la documentación necesaria para facilitar la integración de las aplicaciones de la organización que va a hacer uso de ***VideoID*** con las librerías (SDKs) que implementan la experiencia de usuario, tanto para Web (SDK JavaScript) como para aplicaciones nativas (SDK Android, SDK iOS) así como toda la documentación al respecto del API del servicio de ***VideoID***.

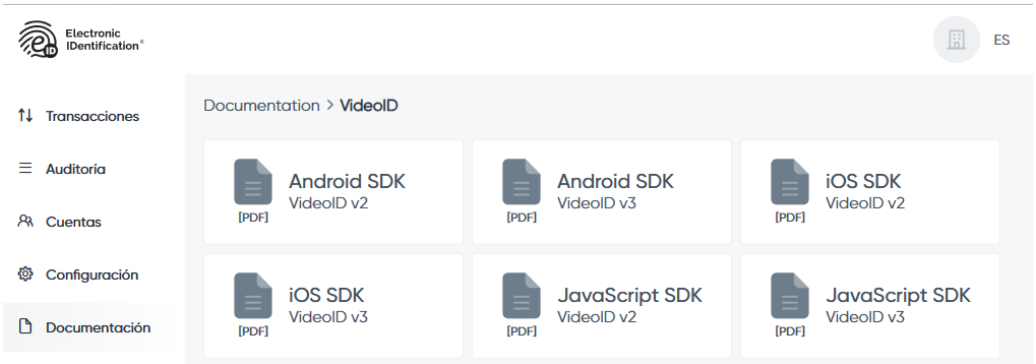


Figura 2 – Documentación accesible desde Dashboard para el servicio VideoID

   c. **Aplicación de video identificación**: ***VideoID***

      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 CCN-STIC 140.F11 [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 CCN-STIC 140.F11 [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: activación de prueba de vida, detección de suplantación de identidad, detección de holograma, y los siguientes elementos del documento de identidad: Integridad de datos, superficie reflectante, copia en blanco y negro, documento expirado, comparación entre anverso y reverso y otras anomalías en el documento.
- **Todos estos aspectos de seguridad no deben ser modificados por la organización que adquiere el producto.** El prestador del servicio proporcionará la configuración adecuada al nivel de seguridad requerido por la guía CCN-STIC 140.F11 [REF1]. Más información al respecto puede ser consultada en el documento "*VideoID Settings*" [REF3].

2. OBJETO Y ALCANCE

6. El objetivo del presente documento es detallar **la configuración de seguridad del servicio ElectronicID VideoID High Solution 3.0 (*VideoID)*** para que su funcionamiento cumpla con los estándares de calidad y los Requisitos Fundamentales de Seguridad (RFS) de la guía CCN-STIC 140.F11 [REF1].

7. ***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.

3. ORGANIZACIÓN DEL DOCUMENTO

8. El presente documento está organizado en diferentes apartados, según las tareas y acciones a tener en cuenta en cada momento del ciclo de vida del servicio:

    a. **Apartado 4. Despliegue e integración.** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de despliegue e integración del servicio.

    b. **Apartado 5. Configuración del Servicio.** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, con el fin de disponer de una configuración segura y que cumpla los requisitos exigidos en la guía CCN-STIC 140.F11 [REF1].

    c. **Apartado 6. Operación y mantenimiento.** En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

    d. **Apartado 7.** Este apartado contiene la documentación a la que se ha hecho referencia a lo largo de este documento.

    e. **Apartado 8.** Este apartado contiene las abreviaturas que han sido empleadas a lo largo de este documento.

4. FASE DE DESPLIEGUE E INTEGRACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

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

   https://www.electronicid.eu/es/contact-us [REF10]

10. La experiencia de usuario se ofrece a través de tres SDKs equivalentes que el cliente integra en sus aplicaciones, bien Web, bien nativas (iOS y Android):

    a. Web: Biblioteca de JavaScript, para aplicaciones que se ejecutan en un navegador web. Funciona en ordenadores de sobremesa, portátiles, teléfonos móviles y tabletas.

    b. iOS: para aplicaciones nativas de dispositivos con Sistemas Operativos iOS. Funciona en teléfonos móviles y tabletas.

    c. Android: para aplicaciones nativas de dispositivos con Sistemas Operativos Android. Funciona en teléfonos móviles y tabletas.

11. Para más información acerca de las versiones de Android, iOS y navegadores web soportadas, se recomienda consultar el documento "*VideoID - Requirements*" [REF7].

12. 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 al *Tenant AWS* asignado a la organización, y que dispone de la siguiente información:

    a. API Token necesario para configurar y gestionar todas las llamadas al API.

    b. Usuario/contraseña para el acceso al *Dashboard*, donde se encuentra toda la documentación necesaria para la integración con las diferentes aplicaciones de la organización que adquiere el servicio: Cliente JavaScript (*SDK Web*), SDK Android y SDK iOS.

    c. URLs de acceso a los diferentes entornos, tanto de pruebas de aceptación de usuario como entorno de explotación.

    d. Entorno de Pruebas de aceptación de usuario: Entorno en el que el cliente realiza sus pruebas de integración previas a la puesta en marcha del servicio.

    e. Entorno de explotación: Entorno de operación del servicio.

    f. API Token y URL de pruebas de la Autoridad de Registro, con la que la organización podrá realizar pruebas de integración y aceptación de la solución previas a la puesta en marcha del servicio.

4.2 ENTORNO DE INSTALACIÓN SEGURO

13. El entorno operacional del servicio VideoID está compuesto por una *Virtual Private Cloud* de Amazon donde se encuentran desplegados los módulos que componen el sistema (*Dashboard, VideoID* y Autoridad de Registro) junto con otros servicios de AWS, en el centro de datos AWS Irlanda (*AWS EU Ireland Region — eu-west-1*).

4.3 REGISTRO Y LICENCIAS

14. **VideoID** no requiere ningún tipo de licencia de instalación, ya que se ofrece en modo SaaS (*Software as a Service*). Las credenciales necesarias para su empleo seguro son entregadas a la organización por el proveedor de servicio en la reunión celebrada para tal fin, tal y como se indica en el apartado 4.1 del presente documento.

4.4 CONSIDERACIONES PREVIAS

15. El servicio VideoID está accesible de forma segura a través del protocolo HTTPS con TLSv1.2 o superior, por lo que es necesario que la organización cliente disponga de conexión a internet.
16. 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.
17. En caso de que el cliente quiera recibir notificaciones provenientes del proveedor del servicio, deberá habilitar una URL:puerto de recepción en su plataforma. Dicha URL:puerto deberá ser indicada posteriormente en el Dashboard (configuración de webhooks).

4.5 INTEGRACIÓN

18. La organización que adquiere ***VideoID*** realizará la integración de su plataforma con las APIs del servicio, así como la integración de los SDKs, descritas en la documentación disponible en *Dashboard.* (ver Figura 2).
19. ElectronicID dará soporte en todo el proceso de integración de la solución ***VideoID***, utilizando su aplicación de gestión de incidencias y soporte técnico (*Helpdesk*) para el seguimiento y análisis de las peticiones y comentarios que puedan surgir durante el proceso.

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

20. El servicio ***VideoID*** dispone de una configuración específica establecida por el proveedor del servicio para el cumplimiento de los RFS indicados en la guía CCN-STIC 140.F11 [REF1]. **Esta configuración no debe modificarse por parte de la organización que adquiere el servicio**.

21. En función del SDK (Web, iOS o Android) que sea necesario integrar, se seguirán las instrucciones referidas en el manual correspondiente disponible en *Dashboard*, siempre referido a VideoID v3.

5.2 AUTENTICACIÓN

22. Existen tres (3) tipos de autenticación:

    a. Autenticación backend a backend: Todo cliente dispone de un API Token (descrito previamente) único para garantizar la seguridad de sus comunicaciones, proporcionado por el equipo de soporte de ElectronicID y que le permitirá acceder a las APIs del proveedor (ElectronicID).

    b. Autenticación desde el SDK: token de autorización de un solo uso. Por cada solicitud de nueva videoidentificación que un usuario pueda generar desde la aplicación del cliente, se solicitará desde el backend de cliente hacia el API de ElectronicID (a través del API Token) una autorización de un solo uso, asociada a un identificador de VideoID único, que será el que se maneje desde la aplicación. El cliente hará llegar la autorización a la aplicación, que se lo comunicará al SDK, y dará viabilidad al stream de vídeo. Una vez finalizado el proceso de videoidentificación, este token de autorización de sesión queda inhabilitado y no puede reutilizarse.

    c. Autenticación en Dashboard y Autoridad de Registro: Para llevar a cabo el proceso de login en la Autoridad de Registro (*eID Registration Authority*), así como en el Dashboard, se empleará autenticación mediante usuario y contraseña.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

23. **El servicio VideoID está accesible de forma segura a través del protocolo HTTPS con TLSv1.2 o superior.**

24. El módulo de *Dashboard* permite administrar los siguientes parámetros:

    a. Creación de usuarios de *Dashboard* y asignación de roles.

    b. Habilitación del sellado de tiempo en las transacciones (obligatorio).

    c. Configuración de *Webhooks* (opcional).

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

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

    a) *Administrador*: Este rol dispone de los privilegios necesario para acceder a los registros de auditoría y transacciones, acceder al token de comunicación con el API, crear usuarios y asignar roles para la plataforma Dashboard y acceder a la documentación de implementación y soporte para la integración con el servicio.

    b) *Auditor*: Puede acceder a los registros de auditoría y transacciones.

    c) *Usuario*: Puede acceder a las transacciones.

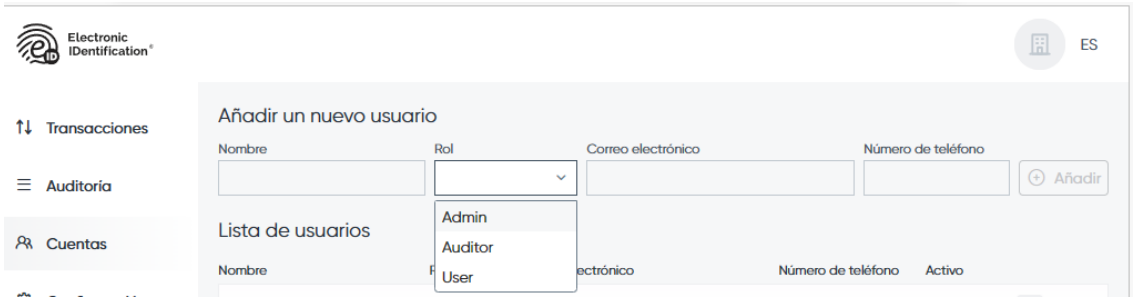


Figura 3 - Listado de usuarios y roles asociados

26. La gestión de las contraseñas en el módulo de Dashboard deberá responder a los siguientes requisitos:

    a. Deberá tener una **longitud mínima de 12 caracteres**.

    b. Debe **contener, al menos, una mayúscula, una minúscula, un número y un carácter especial.**

    c. El producto no permite la reutilización de las últimas 5 contraseñas empleadas por el usuario.

27. El producto no permite establecer un tiempo de validez en días de las contraseñas, tras el cual expiren. La empresa que adquiera el producto deberá **establecer por procedimiento** el cambio de contraseñas cada 2 meses (60 días).

28. El producto no permite establecer un período de tiempo (en días) que deba transcurrir tras el cambio de una contraseña, antes de poder modificarla de nuevo. La empresa que adquiera el producto deberá **establecer por procedimiento** el período mínimo de tiempo para el cambio de una contraseña en 10 días.

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

    a. No se permiten sesiones concurrentes, pudiendo sólo existir una sesión abierta en la aplicación.

    b. Las sesiones se cierran pasado un tiempo de inactividad de 5 minutos.

    c. Se permite un máximo de 3 intentos fallidos, pasados los cuales es necesario esperar 5 minutos para volver a autenticarse.

30. Para más información al respecto, se recomienda consultar el documento "*Dashboard News and Updates*" [REF5].

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

31. 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.

32. Si la organización que adquiere el servicio quiere recibir notificaciones de los eventos de vídeo finalizado, vídeo verificado y vídeo fallido, deberá configurar dichas URLs en el apartado "Configuración" de *Dashboard*.

Figura 4 – Configuración de recepción de notificaciones

33. Para más información al respecto, se recomienda consultar el documento "*Dashboard News and Updates*" [REF5].

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

34. 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 TLSv1.2 o superior.

35. La configuración de los protocolos soportados se realiza directamente en la infraestructura de AWS por parte del proveedor del servicio. No es necesario realizar ninguna configuración adicional por parte de la organización que lo adquiere. Se emplean los protocolos TSLv1.2 y superior.

36. Las suites de cifrado empleadas en la administración del servicio, así como ofrecidas por el servicio ***VideoID*** están admitidas en la guía CCN-STIC 807 [REF2].

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

5.6 GESTIÓN DE CERTIFICADOS

37. No es necesario configurar la gestión de certificados en el servicio ***VideoID***.

5.7 SERVIDORES DE AUTENTICACIÓN

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

5.8 SINCRONIZACIÓN HORARIA

39. No es necesario realizar ningún tipo de configuración para la sincronización horaria, ya que el servicio dispone del NTP (*Network Time Protocol*) proporcionado por AWS.

5.9 ACTUALIZACIONES

40. Al tratarse de un servicio en la nube, ***VideoID*** se actualiza de forma automática con mejoras y correcciones, informando convenientemente a las organizaciones usuarias del servicio de los cambios introducidos en cada *release*.

5.10 AUTO-CHEQUEOS

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

5.11 ALTA DISPONIBILIDAD

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

5.12 AUDITORÍA

5.12.1 REGISTRO DE EVENTOS

43. El servicio recoge los siguientes eventos de auditoría, los cuales están accesibles desde la aplicación Dashboard. Es necesario indicar que el cliente no tiene acceso a los logs del sistema, únicamente a las transacciones que pueden ser consultadas en el módulo Dashboard.

    - *Login* y *logout* del personal autorizado, accesible desde el apartado “Auditoría”.

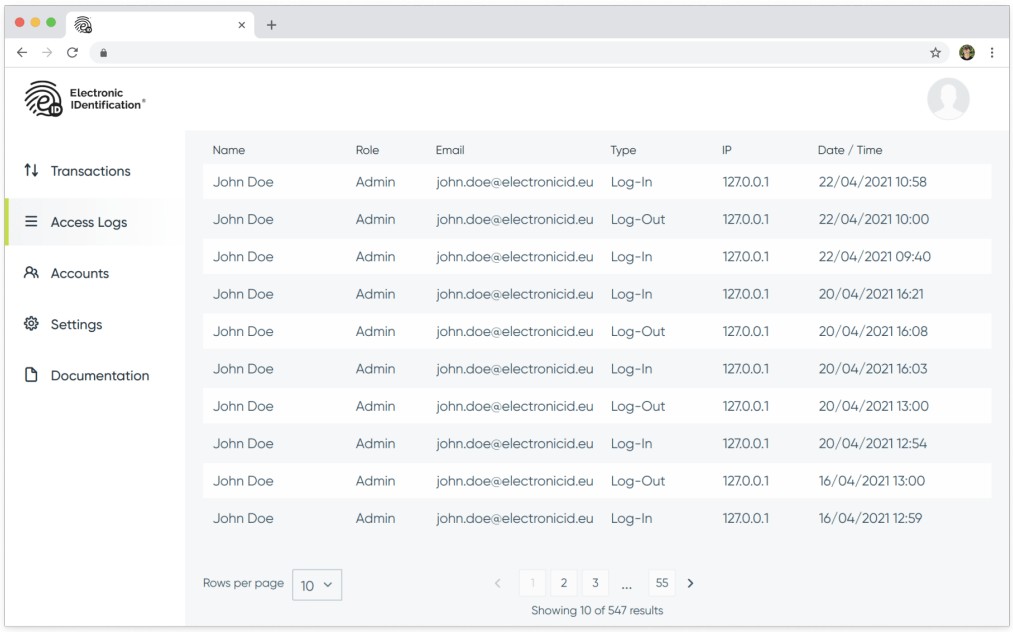


Figura 5 – Ejemplo de registros de *login* y *logout*

- Cambios de configuración en el servicio ***VideoID***, accesible desde el apartado "Transacciones".
- Eventos relacionados con el servicio ***VideoID***:
    a) Finalización de la grabación.
    b) Solicitud de video identificación.
    c) Aprobación de video identificación.
    d) Rechazo de video identificación y sus motivos.

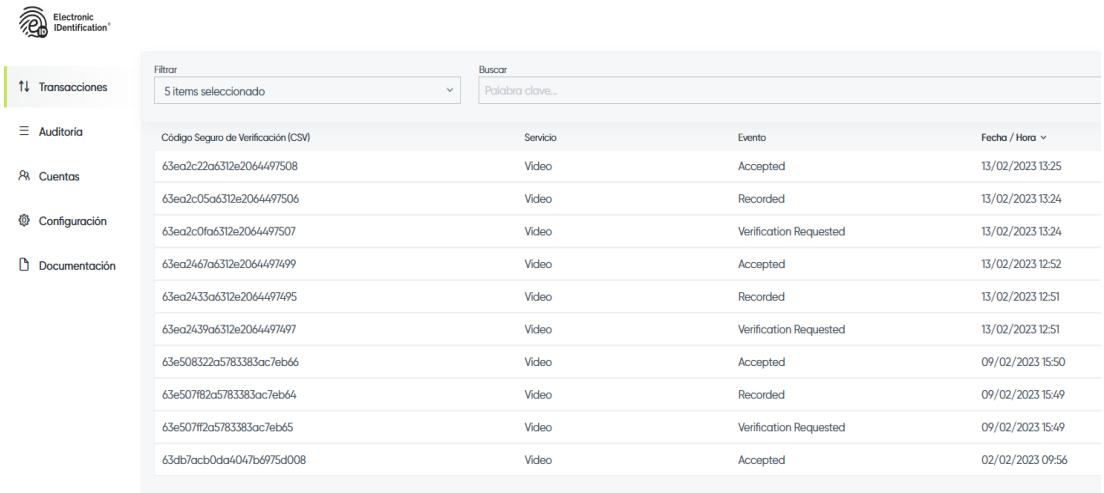


Figura 6 – Ejemplo de eventos del servicio VideoID

44. Así mismo, se recogen los siguientes eventos en los logs del sistema, siendo accesibles sólo por el administrador de la plataforma:
    a. Descripción de errores producidos.

b. Accesos fallidos a la plataforma.

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

46. Los eventos de auditoría disponen de los siguientes campos:

    a. CSV de la transacción (*Verification security code*).

    b. Servicio (Video en este caso).

    c. Tipo de evento (Solicitud verificación, Video identificación Aceptada, Video identificación Rechazada).

    d. Sellado de tiempo.

    e. Fecha y hora del evento.

47. Para más información al respecto, se recomienda consultar el documento "*Dashboard – News and Updates*" [REF5].

5.12.2 ALMACENAMIENTO LOCAL

48. Todos los registros de auditoría se almacenan en la nube, por lo que no es necesario ninguna configuración especial para su almacenamiento local.

5.12.3 ALMACENAMIENTO REMOTO

49. El almacenamiento de los logs se lleva a cabo en la propia infraestructura cloud, no siendo necesaria la configuración de un almacenamiento remoto.

50. Se emplea el protocolo de seguridad TLSv1.2 o superior, así como las suites de cifrado indicadas en el párrafo 36 de este documento.

5.13 BACKUP

51. El servicio ***VideoID*** garantiza un backup de 9 días como mínimo de todos los datos necesarios para el correcto funcionamiento del servicio (credenciales, vídeos realizados, verificaciones, configuraciones, etc.), realizado cada 24 horas, tal y como se encuentra definido en su política de SGSI.

5.14 SERVICIOS DE SEGURIDAD

52. ***VideoID*** dispone de un SOC y un WAF para garantizar la seguridad del servicio. La seguridad de ***VideoID*** es proporcionada por la infraestructura ubicada en la nube.

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

54. 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.

55. El producto cuenta con una serie de mecanismos de comprobación y verificación automática (*security checks*) de los datos recogidos en el proceso de videoidentificación realizado por el usuario final. Para más información acerca de los *security checks*, se recomienda consultar el documento "*VideoID Security Checks*" [REF9].

56. Estos controles de seguridad ya estarán preconfigurados en el momento de la entrega del producto para el cumplimiento de los RFS indicados en la guía CCN-STIC 140.F11 [REF1] y las pruebas indicadas en la IT.014 [REF11]:
    a. Protección frente a ataques en la captura de evidencias
    b. Verificación biométrica
    c. Validación de documentos presentados
    d. Protección frente a ataques de presentación
57. Todas las comprobaciones deberán ser exitosas para considerar que la videoidentificación se ha realizado con éxito.
58. El agente deberá responder a una serie de preguntas de seguridad. Si alguna de las preguntas obtiene una respuesta negativa, el proceso de videoidentificación deberá ser rechazado.
59. Para más información al respecto, se recomienda consultar el documento "*Electronic Identification – Registration Authority 2.0 User Guide*" [REF8].

6. FASE DE OPERACIÓN

60. Para una correcta operación del servicio, la organización deberá mantener la configuración de seguridad del producto, **sin modificar los valores asignados inicialmente**.

61. 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.

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

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

7. REFERENCIAS

64. En este apartado se enumeran la documentación a la que se ha hecho referencia a lo largo de este Procedimiento de Empleo Seguro. Es necesario indicar que los documentos correspondientes a las referencias [REF3] a [REF9] son entregados por el fabricante tras la adquisición del producto.

[REF1] Taxonomía de productos STIC. Anexo F.11. Herramientas de Video identificación.
https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/5461-guia-140-anexo-f-11-herramientas-de-videoidentificacion/file.html

[REF2] Criptología de empleo en el Esquema Nacional de Seguridad
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html

[REF3] *VideoID Settings*

[REF4] *Product Overview*

[REF5] *Dashboard News and Updates*

[REF6] *VideoID Service – Electronic Identification*

[REF7] *VideoID - Requirements*

[REF8] *Electronic Identification – Registration Authority 2.0 User Guide*

[REF9] *VideoID Security Checks*

[REF10] Electronic Identification – Página de contacto
https://www.electronicid.eu/es/contact-us

[REF11] Evaluación de biometría facial. Herramientas de Videoidentificación.

8. ABREVIATURAS

AWS	*Amazon Web Services*
CCN	Centro Criptológico Nacional
CSV	Código Seguro de Verificación
ENS	Esquema Nacional de Seguridad
HTTPS	*HyperText Transfer Protocol Secure*
NTP	*Network Time Protocol*
OTP	*One Time Password*
SDK	*Software Development Kit*
SNMP	*Simple Network Management Protocol*
SOC	*Security Operation Center*
TLS	*Transport Layer Security*
URL	*Uniform Resource Locator*
WAF	*Web Application Firewall*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA SUBSECRETARÍA DE DEFENSA SECRETARÍA GENERAL TÉCNICA SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL