

Guía de Seguridad de las TIC

CCN-STIC 1657

Procedimiento de Empleo Seguro

VerificaID



Octubre 2025



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

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2025
NIPO: 083-26-139-3

Fecha de Edición: Octubre de 2025

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

ÍNDICE

1 INTRODUCCIÓN	3
2 OBJETO Y ALCANCE	4
3 ORGANIZACIÓN DEL DOCUMENTO	5
4 FASE DE DESPLIEGUE E INSTALACIÓN	6
4.1 ENTREGA SEGURA DEL PRODUCTO	6
4.2 ENTORNO DE INSTALACIÓN SEGURO	6
4.3 REGISTRO Y LICENCIAS	6
4.4 CONSIDERACIONES PREVIAS	6
5 INSTALACIÓN.....	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 PROTOCOLOS SEGUROS	10
6.5 GESTIÓN DE CERTIFICADOS	10
6.6 SERVIDORES DE AUTENTICACIÓN	10
6.7 SINCRONIZACIÓN HORARIA	10
6.8 ACTUALIZACIONES	10
6.9 AUDITORÍA	11
6.9.1 REGISTRO DE EVENTOS.....	11
6.9.2 ALMACENAMIENTO LOCAL.....	11
6.10 BACKUP	11
6.11 SERVICIOS DE SEGURIDAD	11
7 FASE DE OPERACIÓN	13
8 REFERENCIAS	14
9 ABREVIATURAS.....	15

1 INTRODUCCIÓN

1. Bewor ofrece un producto de VideoID, **VerificalD.com**, que consiste en una **solución de video identificación para la verificación de identidad**. Esta verificación es llevada a cabo de manera remota, realizando una comparación biométrica de la persona que ejecuta el proceso y verificación de la originalidad del documento de identidad.
2. Durante el proceso, para poder realizar las comprobaciones, la persona deberá mostrar el rostro y ambos lados del documento de identidad. La solución de VideoID realiza las siguientes comprobaciones:
 - **Verificación biométrica:** Durante el proceso se ejecuta una comparación biométrica entre la persona y la foto extraída del documento. Como parte de la verificación, se comprueba la prueba de vida mediante un proceso pasivo, no se requiere que el usuario realice movimientos.
 - **Lectura de OCR:** El proceso realiza captura de ambos lados del documento de identidad, sobre estas capturas se ejecuta un proceso de lectura de texto vía OCR que extrae la información del documento.
 - **Veracidad del documento:** Tanto con el análisis de la información extraída en texto como con la detección de holograma, se evalúa si hay intento de fraude, la vigencia del documento y la veracidad de la información extraída.
3. Por otro lado, Bewor también ofrece una aplicación a través de la cual un operador realiza la revisión de las evidencias extraídas del proceso de videoID y la revisión del proceso completo realizado por la persona. Esta aplicación permite aprobar o rechazar cada solicitud recibida, registrando un log de acciones realizadas.

2 OBJETO Y ALCANCE

4. El objeto de este documento es especificar la configuración para el uso de la solución VideoID, **VerificalD.com**, y la aplicación de revisión (CMS) de Bewor.
5. El servicio de VideoID ofrece API que permite su integración con la aplicación del cliente.
6. La solución completa VerificalD.com, que incluye el servicio de videoidentificación, el CMS y la API, ha sido cualificada en el catálogo CPSTIC para categoría ENS ALTA en la familia “Herramientas de videoidentificación”.

3 ORGANIZACIÓN DEL DOCUMENTO

- a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes y durante la instalación del producto.
- b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación 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.
- d) Apartado 7. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4 FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. El uso de la VideoID de Bewor se realiza mediante integración API. Dicha API no dispone de documentación pública. Tanto el API Key, exclusivo para cada cliente, como la documentación técnica de la API, serán facilitados a solicitud expresa, tanto a clientes potenciales como a clientes que ya hayan formalizado contrato.
8. El acceso a la documentación de la API del producto es privado, mediante el usuario y contraseña facilitados al cliente. Además, se realizará una reunión con el equipo técnico que realizará la integración para indicar los requisitos que deben cumplir para el uso del servicio.

4.2 ENTORNO DE INSTALACIÓN SEGURO

9. El entorno donde se ejecuta el servicio se encuentra en VPC (Virtual Private Cloud) de Amazon en el centro de datos de Irlanda (región eu-west-1).
10. El cliente solicita una video identificación a través de la API y como respuesta, recibe una URL a la que la persona accede para realizar el proceso.

```
{
  "success": true,
  "id": "2f44e0b1-4ec6-492c-9182-611272db8c0f",
  "redirect_url": "https://videoid.bewor.com/onboarding/2f44e0b1-4ec6-492c-9182-611272db8c0f",
  "metadata": {
    "user": {
      "id": 17
    }
  },
  "status": "pending"
}
```

Ilustración 1. URL para realizar el proceso de video identificación

4.3 REGISTRO Y LICENCIAS

11. El servicio de VideoID no requiere ningún tipo de instalación, ya que se ofrece en modo SaaS (Software as a Service), con contratos anuales

4.4 CONSIDERACIONES PREVIAS

12. Al ser un servicio en nube, no se requieren consideraciones previas. Para realizar la video identificación se recomienda buena iluminación, poseer un documento nacional de identidad español y, utilizar una cámara 1080P con autoenfoco.
13. Si se desea ser notificado al finalizar el proceso de VideoID, será necesario indicar una URL de callback al crear una solicitud de video identificación. El contenido del payload recibido en el callback indicado se detalla en la documentación técnica de la API, la cual será facilitada junto con el API Key correspondiente al cliente que lo solicite. Adicionalmente, es posible definir una página de OK y una página de KO, a las cuales se redirigirá al usuario según el resultado del proceso. El formato y los parámetros necesarios para configurar estas páginas también se recogen en la documentación técnica.

14. El cliente puede personalizar el proceso de video identificación indicando colores y logotipo como parte de la configuración. Esta información se envía mediante los parámetros correspondientes en la llamada API, en cada solicitud creada. No existe una configuración global, en cada creación de solicitud se debe indicar logotipo y colores. El detalle del formato de dichos parámetros se encuentra disponible en la documentación técnica de la API, entregada junto con el API Key a los clientes que lo soliciten.

5 INSTALACIÓN

15. La VideoID es ofrecida como un API, por lo que no requiere instalación.
16. El cliente debe realizar un proceso de integración, durante el cual, Bewor dará soporte y seguimiento a la integración.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

17. Bewor ofrece la solución completa en un paquete cerrado. El servicio de videoidentificación se ejecuta completamente dentro de la infraestructura del proveedor del servicio, ofreciendo al cliente una URL donde realizar el proceso, por lo que el cliente no debe encargarse de esto.

6.2 AUTENTICACIÓN

18. Cada cliente dispone de un *API Key* único que garantiza la seguridad de sus comunicaciones y le permite acceder a la API. Esta comunicación está protegida mediante un certificado SSL.
19. El acceso a la documentación de la API es mediante correo electrónico y contraseña. El cliente recibe en su correo un enlace a través del cual configura su contraseña de acceso.
20. El acceso al CMS donde el agente puede validar una solicitud se realiza mediante *email* y *contraseña* (ver sección 6.3.2). Además, el agente debe introducir un OTP que recibe en cada proceso de inicio de sesión.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

21. El servicio VideoID es accesible de forma segura a través del protocolo HTTPS con TLS v1.2 o superior.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

22. En el producto existen tres (3) roles:
 - Operador. Encargado de revisar las evidencias y de decidir su aprobación/rechazo. Tiene acceso a la sección del listado de solicitudes realizadas y puede ver el detalle de cada una mientras la solicitud esté pendiente de ser aprobada/rechazada.
 - Auditor. Puede consultar el log de auditoría que va generando la aplicación y el listado de solicitudes realizadas y el detalle de cada una.
 - Administrador. Rol designado para creación de usuarios. Puede consultar el log de auditoría que va generando la aplicación y el listado de solicitudes, sin poder ver el detalle de cada una.
23. El personal autorizado de Bewor es quien posee el usuario Administrador, encargado de crear usuarios y asignarles el rol.
24. El usuario recibe en su email un enlace a través del cual configura su contraseña de acceso. Los requisitos de la contraseña son:
 - Las contraseñas configuradas deben tener, al menos, 12 caracteres
 - Al menos 2 letras
 - Al menos 2 números
 - No puede tener más de 3 caracteres consecutivos

25. El usuario debe cumplir las siguientes obligaciones:
 - No compartir la contraseña
 - No guardar la contraseña en papel o en formato digital
 - Cerrar sesión cuando el puesto de trabajo sea abandonado
 - Modificar la contraseña si hay sospecha de haber sido comprometida
26. La sesión tiene la siguiente configuración:
 - No se permiten sesiones concurrentes.
 - Las sesiones caducan pasado un tiempo de inactividad de 15 minutos.
 - En el caso de 3 intentos fallidos de *login*, es necesario esperar 10 minutos para volver a realizar otro intento.

6.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

27. Las conexiones con el producto se realizarán mediante conexión HTTPS utilizando TLS v1.2 o superior. No es necesario realizar ninguna configuración adicional por parte del cliente.
28. El producto emplea las siguientes ciphersuites, todas admitidas en la guía CCN-STIC 807 [REF2]:
29. Para TLS 1.2:
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
30. Para TLS 1.3:
 - TLS_AES_256_GCM_SHA384
 - TLS_CHACHA20_POLY1305_SHA256
 - TLS_AES_128_GCM_SHA256
31. Para el almacenamiento de credenciales se utiliza un cifrado admitido en la guía CCN-STIC 807 [REF2].

6.5 GESTIÓN DE CERTIFICADOS

32. No es necesario configurar la gestión de certificados.

6.6 SERVIDORES DE AUTENTICACIÓN

33. No es necesario configurar servidores de autenticación.

6.7 SINCRONIZACIÓN HORARIA

34. No es necesario realizar ningún tipo de configuración para la sincronización horaria.

6.8 ACTUALIZACIONES

35. Al ofrecerse un servicio SaaS, la actualización es transparente al cliente. Este es informado de los cambios introducidos en cada actualización.

6.9 AUDITORÍA

6.9.1 REGISTRO DE EVENTOS

36. El servicio almacena los siguientes registros de auditoría:
- Inicio y cierre de sesión
 - Cambio de credenciales
 - Creación de usuario
 - Cambio de permisos a un usuario
 - Visualización de las evidencias de una solicitud
 - Aprobación/Rechazo de una solicitud, en caso de rechazo, se registra el motivo.
37. Además, el servicio registra cada consumo realizado a la API y su resultado.

6.9.2 ALMACENAMIENTO LOCAL

38. Los logs son almacenados en la infraestructura en la nube, no se requiere configuración para almacenamiento local.

6.10 BACKUP

39. Se realiza una copia de seguridad íntegra y de forma separada diariamente. Esta copia se mantiene al menos, durante 7 días. Las copias de seguridad son inmutables y almacenadas en la zona de disponibilidad de EU-West-1

6.11 SERVICIOS DE SEGURIDAD

40. La seguridad del servicio la proporciona la infraestructura de AWS, por lo que el cliente no necesita aplicar ninguna configuración de seguridad.
41. Los controles de seguridad para el cumplimiento de los RFS recogidos en la guía CCN-STIC 140.F11 [REF1] son regulados por Bewor.
42. Para considerar la video identificación válida, todas las verificaciones deben haberse superado con éxito.

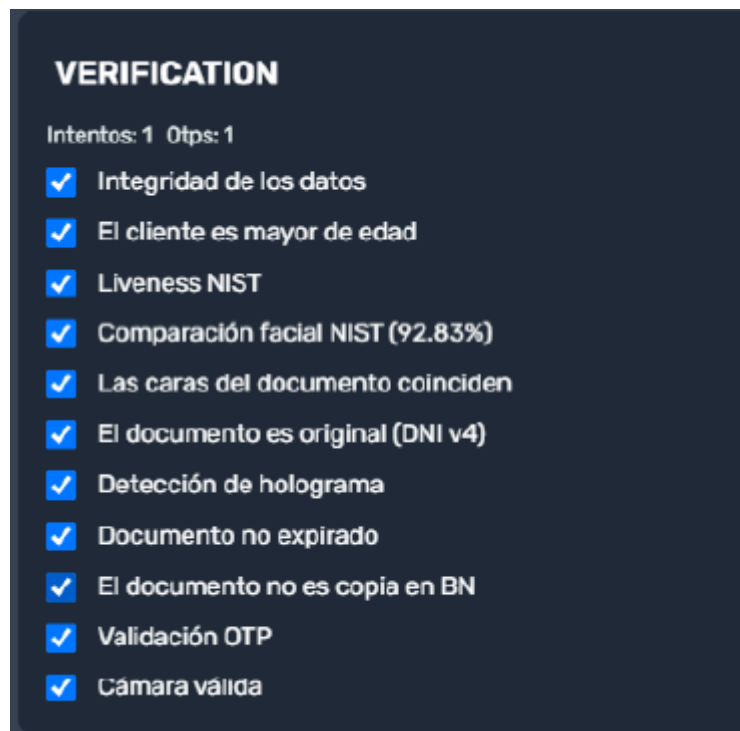


Ilustración 2. Listado de verificaciones realizadas

43. La solicitud entrante a la API debe ser autenticada incluyendo un API Key con la credencial de cliente correspondiente. Se rechazan las solicitudes con el encabezado de clave de API incorrecto.
44. La aplicación cuenta con un servicio que controla el número de peticiones recibidas, bloqueando la IP si se detecta un número alto de peticiones. Hay instalado un cortafuegos para limitar el tráfico entrante.

7 FASE DE OPERACIÓN

45. Para el correcto funcionamiento del producto se debe cumplir las siguientes características:
- El producto debe tener al día las actualizaciones relacionadas con seguridad.
 - Se debe mantener la configuración del producto.
 - Se deben analizar periódicamente los registros de auditoría.
 - Se deben gestionar correctamente los certificados SSL.

8 REFERENCIAS

- [REF1] CCN-STIC 140 Taxonomía de productos STIC. Anexo F.11. Herramientas de Video de identificación.
<https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/5464-guia-140-anexo-f-11m-herramientas-de-videoidentificacion?format=html>
- [REF2] CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad.
<https://www.ccn-cert.cni.es/es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file?format=html>

9 ABREVIATURAS

API	Application Programming Interaces
AWS	Amazon Web Services
CMS	Content Management System
CPSTIC	Catálogo de Productos y Servicios de Tecnologías de la Información y Comunicaciones
ENS	Esquema Nacional de Seguridad
HTTPS	HyperText Transfer Protcol Secure
IP	Internet Protocol
OCR	Optical Character Recognition
OTP	One Time Password
RFS	Requisitos Fundamentales de Seguridad
SaaS	Software as a Service
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
VPC	Virtual Private Cloud

