



CONTRATACIÓN P.A.N.A.P.

**ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVICIOS_
IZENPE S.A.**

PLIEGO DE PRESCRIPCIONES TÉCNICAS RELATIVO A LA CONTRATACIÓN DE HERRAMIENTA DE
VIDEOIDENTIFICACIÓN .

Nº EXPEDIENTE: IZNP_S_002_2024_



Contenido

1	OBJETO	3
2	NECESIDADES A SATISFACER	3
3	CARACTERÍSTICAS TÉCNICAS	4
4	TRANSFERENCIA DE TECNOLOGÍA Y DE CONOCIMIENTO.	10
5	COORDINACIÓN Y REPORTING	10

1 OBJETO

En la actualidad Izenpe cuenta con la solución de Veridas para realizar videoidentificaciones de las personas usuarias para solicitar un certificado digital en la nube denominado BakQ.

El objeto es la contratación por Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A. (en adelante, Izenpe) de una herramienta de videoidentificación para la realización de identificaciones a distancia y que cumpla con los Requisitos Fundamentales de Seguridad (RFS) exigidos por el Centro Criptológico Nacional (en adelante, CCN) de un producto de la familia Herramientas de Videoidentificación de Nivel Alto (Anexo F.11: Herramientas de Videoidentificación) incluido en el apartado de Productos Cualificados del Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC), publicado por el CCN, y que será utilizado en sistemas de información que requieren la aplicación el Esquema Nacional de Seguridad (ENS) con categoría ALTA.

2 NECESIDADES A SATISFACER

La guía RFS del CCN describe dos casos de uso en función de las funcionalidades:

- a) Caso 1. Proceso asistido o síncrono: el operador participa en el propio proceso de identificación *on line* y toma la decisión de forma inmediata.
- b) Caso 2. Proceso desasistido o asíncrono: el operador toma la decisión a posteriori, en función de las evidencias recibidas off line, como proceso de back-office.

El alcance que se requiere para la herramienta a contratar es el Caso 2, proceso desasistido o asíncrono, es decir, toda la recogida de evidencias se realizará mediante interacción entre el solicitante y la herramienta:

1. El operador no interactúa con el usuario, solo consulta y analiza la información, almacenada previamente en los sistemas de información e indexada en la base de datos.
2. El operador accede a un panel o cuadro de mandos en el que tiene acceso a todas las evidencias (imágenes, videos y resultados de las validaciones automáticas) y aprueba o rechaza la identificación en función del análisis realizado de las evidencias.



Operador



3. Este caso de uso no forma parte de la experiencia de usuario: la verificación se realiza en el back-office, a partir de los datos capturados en un proceso videoidentificación anterior.

3 NECESIDADES TÉCNICAS

La herramienta deberá cumplir con los siguientes requisitos técnico:

R1. La herramienta de captura de evidencias ha de proporcionar un API de integración que funcione correctamente al menos en los siguientes navegadores Internet Explorer, Firefox, Chrome y Safari sobre Windows MacOS, Linux, Android e IOS

R2. Las pantallas que se muestren deberán ser responsivas y en cumplimiento con la norma de accesibilidad ETSI EN 301 549.

R3. Los interfaces de las herramientas que se oferten tendrán tener soporte multidioma.

R4. El proceso de identificación se interrumpirá o no se considerará válido cuando concurra alguna de las siguientes circunstancias:

- Existan indicios de falsedad o manipulación del documento de identificación;
- Existan indicios de falta de correspondencia entre el titular del documento y el solicitante;
- La calidad de la imagen y el sonido impidan o dificulten verificar la autenticidad e integridad del documento de identificación y la correspondencia entre el titular del documento y el solicitante
- Las condiciones de la comunicación impidan o dificulten verificar la autenticidad e integridad del documento de identificación y la correspondencia entre el titular del documento y es solicitante;
- Existan indicios de uso de archivos pregrabados;
- Existan indicios de que para la transmisión de video no se ha utilizado un único dispositivo.
- Existan indicios de que la transmisión de video no se ha realizado en tiempo real

R5. Las evidencias se almacenarán en el Centro de Proceso de Datos de Izenpe, por lo que el módulo de gestión que operen las personas operadoras de Izenpe para realizar la validación de las evidencias recogidas no podrá estar en la nube.

R6. El módulo de captura de datos y de procesamiento y comparación (motor biométrico) podrá estar albergado en la nube. Si bien, dicha infraestructura deberá estar dentro del territorio establecido en el Decreto Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones donde se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en territorio español

R7. Si el módulo del R4 se ofrece en modo SaaS se deberá garantizar una disponibilidad superior al 99%

R8. La herramienta debe garantizar que el proceso se ejecuta en unidad de acto, de forma que pueda evidenciarse que se trata de un único proceso en un único dispositivo y en un único acto secuencial en el tiempo, con independencia de que se ejecute en varios pasos.

R9. La herramienta debe aportar mecanismos para garantizar que el proceso de identificación es realizado en tiempo real. En el caso de la grabación de video, este debe realizarse en directo, no se permiten archivos pregrabados.

R10. La herramienta permitirá al agente, durante el proceso o a posteriori, analizar las características biométricas del solicitante y la correspondencia de la información incluida en el documento de identidad con la instantánea o imagen del solicitante.

R11. El sistema biométrico de comparación facial entre el solicitante y la foto del documento de identidad debe haber sido evaluado, según el Face Recognition Vendor Test (FRVT) en la categoría VISABORDER, del NIST y haber obtenido una tasa de FNR (False

Negative Rate) menor o igual al 5% para un FPR (False Positive Rate) de menor o igual a 1/1 000 000. La base de datos utilizada para la prueba debe ser la utilizada por el NIST en 2020 o superior.

R12. La herramienta permitirá la videoidentificación de ciudadanos extranjeros, mediante Tarjeta de Identidad de Extranjero, pasaporte o documento oficial de identidad extranjero expedido por las autoridades del país de origen, acompañado, en su caso, del Número de Identidad de Extranjero, siempre que incluya una fotografía, cuyas características de seguridad sean comprobables en el proceso de identificación remota por vídeo de forma que se garantice la detección de falsificaciones y manipulaciones

R13. La solución debe establecer medidas técnicas para detectar que la persona está viva a través de pruebas activas o pasivas. El sistema biométrico deberá implementar una detección de ataque de presentación biométrica PAD, acorde a la metodología definida por el CCN para los laboratorios acreditados dentro de su esquema.

R14. La herramienta implementará mecanismos de detección de manipulaciones del documento de identidad para todas aquellas características que sean apreciables visualmente. Algunas posibles medidas son:

- Características del documento: tamaño, patrón, diseño, espaciado entre caracteres y tipografía del documento.
- Medidas de seguridad: hologramas, imágenes laser variable, etc....

R15. La herramienta debe ser capaz de verificar que la fecha de validez del documento no ha expirado.

R16. La herramienta debe ser capaz de verificar que las fechas incluidas en el documento presentan una relación lógica.

R17. La herramienta debe ser capaz de validar que el anverso y el reverso del documento corresponden al mismo documento.



R18. La herramienta deberá comprobar la integridad de los datos de la zona de inspección visual (VIZ) con la MRZ (zona de lectura mecanizada) ...

R19. La herramienta permitirá al operador verificar visualmente que las características del documento de identidad incluidas en el R14.

R20. La herramienta permitirá a un operador supervisar a posteriori el proceso de identificación grabado y le permitirá comprobar las evidencias generadas del documento.

R21. Se constatará de manera fehaciente la fecha y hora de la grabación mediante el uso de un sello cualificado de tiempo de Izenpe.

R22. La herramienta emitirá un scoring biométrico facial entre la cara de la persona que se está identificando y la de la imagen del documento o la proveniente de una fuente auténtica, cuyo valor mínimo se podrá indicar desde Izenpe.

R23. La herramienta obtendrá y gestionará la conservación de la captura del anverso y del reverso del documento de identidad, que deberá tener la calidad suficiente que permita verificar la información.



R24. La herramienta debe generar información de auditoría al comienzo y finalización de las funciones de auditoría y cuando se produzca alguno de los siguientes eventos:

- Login y logout de personal autorizado.
- Cambio en las credenciales de usuarios administradores del servicio.
- Cambios en la configuración.
- Cualquier otro evento relacionado con el proceso de identificación y validación del documento de identidad.

R25. Los registros de auditoría deben contener, al menos, la siguiente información: fecha y hora del evento, tipo de evento identificado, resultado del evento, usuario que produce el evento (si aplica).

R26. La herramienta debe registrar la cadena de custodia de la verificación, tanto la parte automática como la acción del operador.

R27. La herramienta debe registrar el resultado de los procesos de verificación junto con el motivo de rechazo, en caso de tratarse de un resultado negativo.

R28. Los registros de auditoría solo podrán ser consultados y eliminados por usuarios con el rol de auditor o de forma automática cuando se alcance el tiempo máximo configurado en el producto.

R29. La herramienta deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas o entre distintas partes del producto empleando funciones, algoritmos y protocolos que estén de acuerdo a lo establecido en la guía CCN-STIC-807 (p.ej.: HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, etc.).

R30. La herramienta deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones administrativas.



R31. La herramienta tendrá la capacidad de definir tres tipos de roles de validador, administración configurador y auditor.

R32. La herramienta deberá identificar y autenticar a cada usuario antes de otorgar acceso. Dicha autenticación se realizará con sistemas de doble factor (p ej certificado electrónico)

R33. La herramienta deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.

R34. La herramienta deberá proteger de lectura y modificación no autorizada las credenciales de autenticación.

R35. La herramienta debe bloquear o cerrar la sesión de un usuario después de un determinado periodo de tiempo de inactividad.

R36. En el caso en que la herramienta almacene credenciales y/o datos sensibles, éstos no deberán almacenarse en claro

R37. En caso de que el módulo de captura de datos y de procesamiento y comparación (motor biométrico) deba almacenar de forma temporal datos biométricos, éstos datos no podrán permanecer más de 30 minutos, se garantizará la confidencialidad de dichos datos en todo momento, y se garantizará también el borrado definitivo de los mismos una vez finalizado el proceso.

R38. La herramienta ha de estar incluida dentro del listado de CCN en el apartado de Herramientas de Videoidentificación para sistemas de información que requieren la aplicación el Esquema Nacional de Seguridad (ENS) con categoría ALTA



4 ENTREGABLES Y PLAZOS.

El adjudicatario deberá proporcionar dos entornos (desarrollo y producción) totalmente operativos en un plazo de un mes desde la firma del contrato. En el momento de la adjudicación se proporcionarán los requisitos en cuanto a sistemas (servidores, Base de Datos, comunicaciones requeridas....) para comenzar con el aprovisionamiento de los mismos por parte de Izenpe.

Se entregará la siguiente documentación:

- Documento de arquitectura de la solución.
- Manual de integración con los APIs de las herramientas ofertadas.
- Manual de administrador, auditor y validador de la herramienta de revisión de evidencias que se albergará en Izenpe.
- Manual de instalación de producto

El adjudicatario deberá realizar la formación de los técnicos designados, en todos aquellos aspectos que Izenpe crea oportunos y que sean de directa aplicación a los servicios requeridos.

5 DEVOLUCIÓN DEL SERVICIO

El adjudicatario deberá asumir sin coste para Izenpe el plan de transición para hacerse cargo del servicio, donde se incluye la implantación de la nueva solución en el Centro de Proceso de Datos de Izenpe e integración con flujo de Izenpe. Al final del servicio el adjudicatario deberá planificar y ejecutar el plan de devolución del servicio en caso de cambio de proveedor. El coste del plan de devolución del servicio está incluido en el presupuesto del contrato.

El adjudicatario deberá hacer una eliminación segura de toda la información del servicio una vez éste haya sido transferido.

6 COORDINACIÓN Y REPORTING

La coordinación y reporting se realizará de la forma siguiente:

- Trimestralmente, el coordinador designado por el adjudicatario presentará a Izenpe un informe de indicadores relativos a los servicios prestados.
- En el caso del soporte e incidencias se presentarán informes que reflejen el tiempo de respuesta y el dedicado. Debe existir una traza de las acciones y pruebas realizadas y documentación sobre cómo resolver una duda o incidencia similar (FAQS, base de conocimiento, notas técnicas etc.)
- Además, se deberá aportar documentación de diseño sobre las modificaciones que tengan impacto en la configuración y administración de la plataforma. Izenpe deberá aprobar previamente esos cambios. Se incluirán todos los cambios referentes a seguridad, procedimientos, etc.



- La empresa adjudicataria incluirá dentro del servicio una herramienta para la gestión de las tareas a realizar en el servicio que permita la gestión de las mismas. Así mismo, contará con un teléfono 8x5 para la atención de las incidencias que puedan surgir.

Toni Sáez González	Izaskun Urrestarazu Amundarain
Técnico Responsable del Contrato	Izenpe