

Guía de Seguridad de las TIC CCN-STIC 1646

Procedimiento de Empleo Seguro MobbScan



Julio de 2026

Edita:



Centro Criptológico Nacional, 2026



CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-
S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.07.28 09:46:14
+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

1 INTRODUCCIÓN	4
2 OBJETO Y ALCANCE	4
3 ORGANIZACIÓN DEL DOCUMENTO	6
4 FASE PREVIA A LA INSTALACIÓN	7
4.1 ENTREGA SEGURA DEL PRODUCTO	7
4.2 ENTORNO DE INSTALACIÓN SEGURO	7
4.3 REGISTRO Y LICENCIAS	7
4.4 CONSIDERACIONES PREVIAS	8
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN	8
5 FASE DE INSTALACIÓN	11
6 FASE DE CONFIGURACIÓN	12
6.1 MODO DE OPERACIÓN SEGURO	12
6.2 AUTENTICACIÓN	12
6.2.1 AUTENTICACIÓN DE USUARIOS	12
6.2.2 AUTENTICACIÓN ENTRE COMPONENTES DEL PRODUCTO	12
6.2.3 AUTENTICACIÓN CON UN TERCERO DE CONFIANZA	13
6.3 ADMINISTRACIÓN DEL PRODUCTO	13
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA	13
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES	16
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS	17
6.5 GESTIÓN DE CERTIFICADOS	17
6.6 SERVIDORES DE AUTENTICACIÓN	18
6.7 SINCRONIZACIÓN	18
6.8 ACTUALIZACIONES	18
6.9 AUTO-CHEQUEOS	18
6.10 ALTA DISPONIBILIDAD	19
6.11 AUDITORÍA	19
6.11.1 REGISTRO DE EVENTOS	19
6.11.2 ALMACENAMIENTO LOCAL	21
6.11.3 ALMACENAMIENTO REMOTO	21
6.12 BACKUP	21
7 FASE DE OPERACIÓN	22
7.1 HERRAMIENTA DE ASISTENCIA AL OPERADOR	23
7.1.1 ACCESO DEL OPERADOR AL PORTAL DEL AGENTE	23
7.1.2 REVISIÓN DE EVIDENCIAS	24
7.2 MANTENIMIENTO	27
8 REFERENCIAS	28
9 ABREVIATURAS	29

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Arquitectura de MobbScan	5
Ilustración 2. Componentes del entorno de operación	9
Ilustración 3. Gráfica para la configuración de umbrales de decisión biométricos	16
Ilustración 4. Acceso del operador	23
Ilustración 5. Portal del agente	24

Ilustración 6. Cambio de disponibilidad del operador	24
Ilustración 7. Revisión de evidencias.....	25
Ilustración 8. Interfaz de Aceptación/Rechazo	27
Ilustración 9. Interfaz de razón de rechazo	27

1 INTRODUCCIÓN

MobbScan es una herramienta que permite la autenticación y videoidentificación remota de usuarios de manera segura y confiable. Para ello incorpora una serie de módulos que posibilitan recabar y validar la información personal de un usuario mediante el análisis de su documento de identidad y posteriormente comprobar mediante biometría facial que la persona que realiza el trámite es la propietaria del mismo.

Durante todo el proceso se generan una serie de muestras y evidencias que son almacenadas temporalmente de manera segura hasta que un agente autorizado pueda revisarlas y validarlas a través de un portal web que asiste en esa tarea (proceso desasistido o asíncrono).

El sistema utiliza tecnologías de inteligencia artificial para realizar comprobaciones sobre el documento de identidad que permitan determinar su integridad (validez de los datos) o posible uso fraudulento (uso de copias o reproducciones digitales).

El motor biométrico cuenta con tecnologías avanzadas que permiten detectar intentos de ataques de suplantación mediante el uso de instrumentos como máscaras, pantallas, caracterización o *deepfake*. Las conclusiones de estos análisis se muestran igualmente al agente encargado de tomar la decisión sobre la validez del proceso para facilitar su tarea y añadir una capa extra de seguridad y robustez a la solución.

2 OBJETO Y ALCANCE

El objetivo de este documento es servir de guía para la instalación y configuración segura de MobbScan (v2.35), incluyendo todos los componentes que lo conforman.

MobbScan se compone de tres módulos principales:

- a) **Cliente:** aplicación que guía al usuario por las diferentes etapas del proceso de videoidentificación, incluyendo el escaneo del documento de identidad, la verificación mediante biometría facial y la revisión y envío de información.
- b) **Servidor:** aplicación que incorpora toda la lógica del sistema y gobierna las comunicaciones entre los diferentes módulos. Es la encargada de almacenar las muestras y realizar comprobaciones sobre ellas, comunicarse con las bases de datos y servicios externos, asignar los procesos de revisión a los agentes o implementar la capa de seguridad del sistema.
- c) **Agente:** aplicación que asiste al agente en la toma de decisión sobre la validez de un proceso de videoidentificación. Muestra las evidencias y comprobaciones realizadas en el proceso de una manera sistematizada para minimizar la probabilidad de errores y mejorar su productividad. Incorpora igualmente un espacio para la auditoría y la gestión de operaciones sólo accesible para aquellos perfiles autorizados.

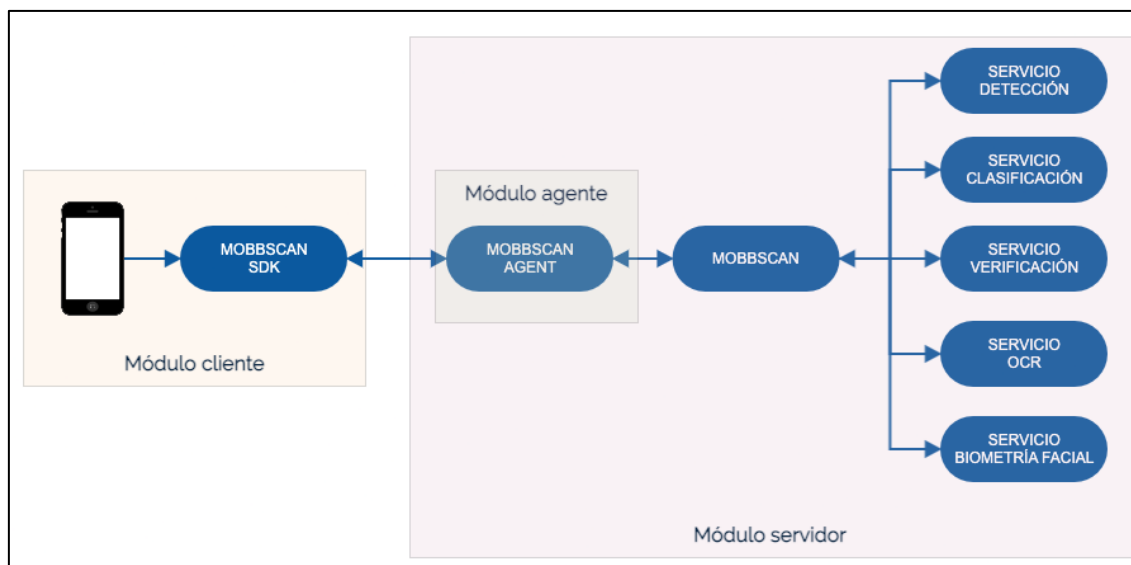


Ilustración 1. Arquitectura de MobbScan

Los requisitos hardware del entorno operacional son los siguientes:

- a) **Módulo cliente:** MobbScan dispone de SDKs nativos para diferentes entornos (Android [REF2] e iOS [REF3]) que incorporan idénticas funcionalidades. En el caso de iOS, el modelo de dispositivo que cumple con las condiciones técnicas mínimas es iPhone7 (2016), aunque se recomienda la ejecución con un modelo iPhone XR (2018) o superior. En el caso de Android se recomienda el uso mínimo de la versión Android 10 y una cámara con resolución FullHD o 4K.
- b) **Módulo servidor:** Alberga toda la lógica de negocio de MobbScan, además del módulo agente. MobbScan utiliza el ecosistema Amazon Web Services (AWS) como su entorno operacional fundamental. De forma concreta, MobbScan hace uso de los siguientes servicios:
 - i) **AWS EC2 (Elastic Cloud Computing):** creación y administración de servidores virtuales, balanceadores de carga y *gateways*, incluyendo las políticas de despliegue y escalado para garantizar la disponibilidad del servicio.
 - ii) **AWS RDS (Relational Database Service):** creación y administración de instancias de bases de datos compatible con diferentes motores.
 - iii) **AWS EFS (Elastic File System):** almacenamiento de sistema compartido de archivos NFS para cargas de trabajo Linux.
 - iv) **AWS KMS (Key Management System):** creación, administración y control de claves criptográficas.
 - v) **AWS CloudWatch:** monitorización y centralización de logs.

El producto MobbScan ha sido incluido en el CPSTIC. Para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF7].

3 ORGANIZACIÓN DEL DOCUMENTO

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 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 PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

MobbScan es una aplicación *cloud*, por lo tanto, no es necesario el envío de ficheros de instalación. Una vez acordado con el equipo comercial la fecha de inicio del servicio para un nuevo cliente, un administrador de sistemas del equipo de operaciones de Mobbeel dará de alta a un perfil de administrador configurador. Este administrador configurador designado por el nuevo cliente recibirá un correo electrónico con remitente noreply@mobbbeel.com en el que aparecerá un enlace de invitación para que pueda realizar el primer acceso al módulo del agente.

En este primer acceso deberá establecer una contraseña que cumpla con los requisitos de seguridad establecidos en la guía CCN-STIC 807 [REF1] para autenticación de usuarios internos nivel ALTO. Se recomienda en este punto que se active el segundo factor de autenticación (2FA) para aumentar la seguridad del proceso.

Una vez finalizada la configuración del acceso la cuenta quedará operativa y el administrador configurador será el encargado de crear y gestionar las cuentas de nuevos usuarios.

Respecto a la parte cliente, las SDKs móviles nativas serán entregadas de forma segura, en concreto a través del envío de un enlace por correo electrónico a la cuenta establecida. Dicho enlace (protegido con contraseña de un solo uso y fecha de caducidad) permitirá descargar desde el repositorio privado de Mobbeel (nextcloud.mobbbeel.com) las librerías correspondientes.

4.2 ENTORNO DE INSTALACIÓN SEGURO

Tal como se indicó anteriormente MobbScan es una solución *cloud* por lo que no es necesario llevar a cabo un proceso de instalación personalizado. Toda la infraestructura se encuentra desplegada en el entorno de Amazon Web Services EU y es administrada en exclusiva por Mobbeel.

En lo relativo al módulo cliente, el integrador deberá importar en su aplicación las SDKs nativas de MobbScan para implementar las funcionalidades que permiten la operativa del proceso de videoidentificación. En el apartado 5 FASE DE INSTALACIÓN se encuentran los detalles para realizar este proceso.

4.3 REGISTRO Y LICENCIAS

Como servicio *cloud* no es necesario instalar un fichero de licencia y el control de usos y acceso se realizará a través de la pantalla de login y de las credenciales otorgadas en la fase de entrega del producto. Tal como se describe en el apartado 4.1 ENTREGA SEGURA DEL PRODUCTO se generará un perfil de administrador configurador que permitirá a su vez la creación de otros perfiles a voluntad del cliente. Respecto a la parte cliente, las SDKs nativas necesitan incluir en su configuración una clave de licencia para operar. El fichero de clave podrá descargarse desde el repositorio privado corporativo (M365) de Mobbeel a través de un enlace protegido con contraseña de un solo uso y fecha de caducidad.

4.4 CONSIDERACIONES PREVIAS

No es necesario realizar ningún tipo de configuración previa ya que el entorno *cloud* se encuentra gestionado por los administradores de sistemas de Mobbeel y está diseñado con parámetros que permiten una operación segura y fiable. La arquitectura presenta un esquema de alta disponibilidad que se adapta en tiempo real a la demanda del servicio por lo que no es necesario realizar una provisión de recursos previa. El único aspecto a tener en cuenta es el cumplimiento con los requisitos mínimos del servicio:

- a) **Canales seguros de comunicación para el intercambio de peticiones:** HTTPS con versión mínima de TLS igual o superior a 1.2 (las inferiores serán rechazadas automáticamente).
- b) **Versiones mínimas de navegadores web para el módulo agente:**
 - i) MacOS:
 - Safari 11
 - Chrome 41
 - Firefox 50
 - Opera 40
 - ii) Windows:
 - Chrome 50
 - Firefox 49
 - Opera 40
- c) **Versiones mínimas de SO para las SDK cliente nativas:**
 - i) Android: 4.1 o posterior. Cámara con autofocus.
 - ii) iOS: 11.0 o superior. Cámara con autofocus.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

En la figura se muestran todos los componentes del entorno de operación de MobbScan. Tal como se ha comentado anteriormente, se trata de un servicio *cloud* mantenido por Mobbeel, por lo que no es necesario que el cliente lleve a cabo ningún tipo de configuración o personalización desde el punto de vista de la arquitectura general del sistema.

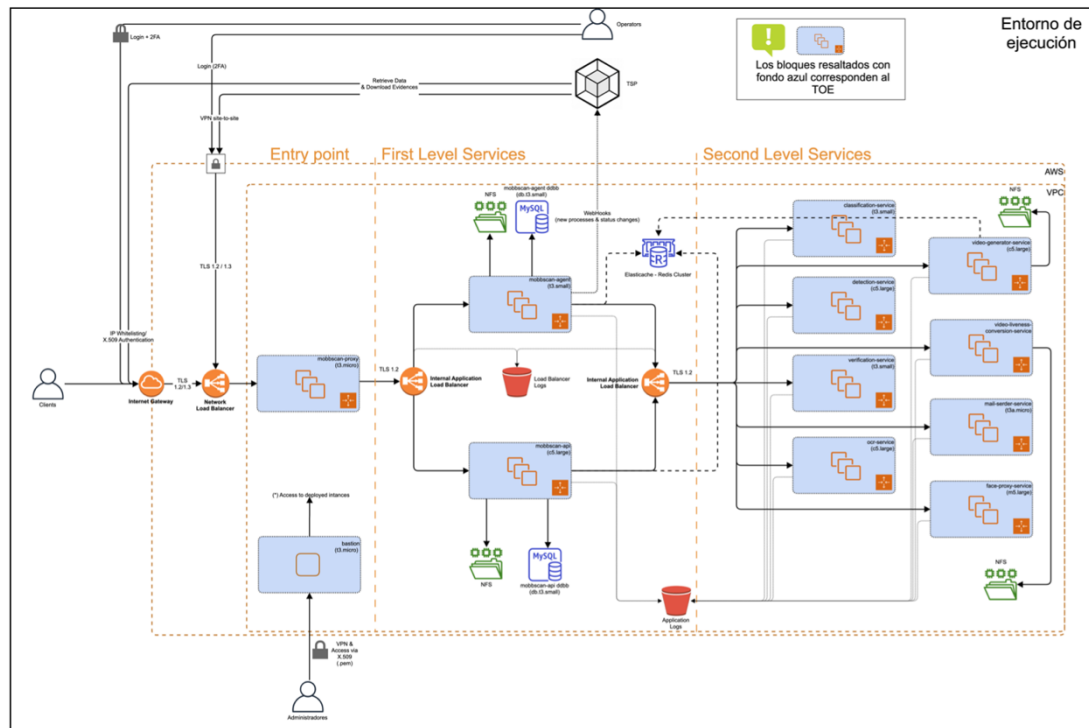


Ilustración 2. Componentes del entorno de operación

Descripción de los componentes principales del entorno de ejecución.

El producto se despliega sobre una VPC en AWS, segmentada en tres niveles funcionales y protegida en su perímetro mediante un Internet Gateway y un Network Load Balancer. El acceso de clientes se realiza vía TLS 1.2/1.3 con IP Whitelisting y autenticación X.509; los operadores acceden mediante Login + 2FA sobre VPN site-to-site, y los administradores a través de un *bastion* con autenticación X.509 (.pem).

a) Punto de entrada (Entry point):

- i) **mobbscan-proxy**: Proxy de entrada que recibe el tráfico del balanceador de red y lo enruta hacia los servicios de primer nivel mediante TLS 1.2.

b) Servicios de primer nivel (First Level Services):

- i) **mobbscan-api**: Servicio principal de exposición de la API del producto. Dispone de base de datos propia (*mobbscan-api ddbb*, MySQL) y almacenamiento NFS.
- ii) **mobbscan-agent**: Componente de orquestación y gestión de procesos, con base de datos propia (*mobbscan-agent ddbb*, MySQL) y NFS. Emite *WebHooks* (nuevos procesos y cambios de estado) hacia el TSP.
- iii) **Internal Application Load Balancers**: Distribuyen el tráfico interno entre las capas de primer y segundo nivel (TLS 1.2), registrando la actividad en *Load Balancer Logs*.

c) Servicios de primer nivel (First Level Services). Microservicios especializados que ejecutan las funciones biométricas y de tratamiento documental:

- i) **classification-service**: Clasificación de documentos.
- ii) **detection-service**: Detección de documentos/elementos.
- iii) **verification-service**: Verificación de identidad.
- iv) **ocr-service**: Extracción de datos por OCR.
- v) **face-proxy-service**: Procesamiento facial.

- vi) **video-generator-service** y **video-liveness-conversion-service**: Generación y conversión de vídeo para prueba de vida.
- vii) **mail-sender-service**: Notificaciones por correo.
- d) **Componentes transversales de soporte**:
 - i) **Elasticache y Redis Cluster**: Caché y gestión de estado compartido entre servicios.
 - ii) **NFS**: Almacenamiento de ficheros compartido entre las distintas capas.
 - iii) **Application Logs / Load Balancer Logs**: Registro centralizado de actividad y trazabilidad.
 - iv) **Bastion**: Único punto de acceso administrativo a las instancias desplegadas.

Nota: los bloques resaltados con fondo azul (mobbscan-proxy, mobbscan-api, mobbscan-agent, los servicios de segundo nivel y el bastion) corresponden al TOE (objeto de la evaluación); el resto constituye la infraestructura del entorno operacional.

5 FASE DE INSTALACIÓN

Para implementar un flujo de *onboarding* digital (proceso de videoidentificación), el integrador deberá importar en su aplicación la SDK nativa correspondiente al sistema operativo de interés (Android [REF2] o iOS [REF3]). En la documentación pública del producto es posible encontrar todos los detalles técnicos necesarios para hacer uso de las funcionalidades que ofrece la herramienta. Esto incluye la configuración general, gestión de dependencias o la personalización de apariencia.

Cada paso está documentado con ejemplos de código para facilitar el proceso de integración, pero ante cualquier problema el equipo de soporte de MobbScan prestará la ayuda necesaria.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

El módulo del agente se encuentra configurado para operar dentro de los requisitos marcados por la guía CCN-STIC 140.F11 [REF4] por lo que no es necesario que el integrador lleve a cabo ninguna acción.

En el caso del módulo cliente, el integrador deberá hacer uso de los recursos de las SDKs nativas que permiten implementar un flujo de *onboarding* siguiendo los requisitos de la guía CCN-STIC 140.F11. Esto supone incorporar los siguientes pasos:

- a) Detección y escaneo del documento de identidad.
- b) Captura de una imagen facial para la comparación biométrica y la detección de ataques de presentación.
- c) Prueba de vida con desafío aleatorios.

Todo el proceso es grabado de inicio a fin en un vídeo que se envía posteriormente al portal del agente como una evidencia más cumpliendo con lo establecido en la guía CCN-STIC 140.F11.

El integrador únicamente tendrá que configurar la SDK en modo vídeo desatendido (*unattended video*) y el propio sistema se encargará de establecer el flujo de onboarding descrito anteriormente. En la documentación pública del producto para Android [REF2] e iOS [REF3] se detalla cómo realizar el proceso con ejemplos de código.

Una vez configurado el flujo de *onboarding*, MobbScan se encargará de almacenar y procesar todas las evidencias para su posterior envío al portal del agente para su revisión por parte de un operador.

6.2 AUTENTICACIÓN

6.2.1 AUTENTICACIÓN DE USUARIOS

Para acceder al portal del agente el usuario deberá utilizar la contraseña que especificó al registrarse como usuario autorizado. Para añadir una capa extra de seguridad es posible solicitar un segundo factor de autenticación (2FA) a través del envío de un código OTP al correo electrónico.

Cuando un administrador configurador da de alta a un nuevo operador en el sistema tendrá la opción de solicitar un 2FA. En ese caso el operador recibirá en su cuenta de correo un código OTP que deberá introducir **durante el proceso de registro**.

6.2.2 AUTENTICACIÓN ENTRE COMPONENTES DEL PRODUCTO

Las SDKs nativas deben aportar la clave de licencia proporcionada según lo detallado en el proceso 4.3 REGISTRO Y LICENCIAS para ser inicializadas y poder operar. Una vez listas, intercambiarán información con el módulo agente (por ejemplo, para el envío de evidencias) utilizando canales seguros (HTTPS con TLS ≥ 1.2).

6.2.3 AUTENTICACIÓN CON UN TERCERO DE CONFIANZA

En caso de querer permitir conexiones externas con un tercero de confianza (por ejemplo, para almacenar y custodiar las evidencias de un proceso de videoidentificación) se utilizará un mecanismo de Webhooks (HTTPS). El TSP podrá realizar llamadas a la API HTTPS cuyo acceso estará restringido por uno o varios de los siguientes mecanismos:

- a) Listas de acceso restringidas (IP Whitelisting).
- b) MutuaL TLS a través de certificados X.509.
- c) VPN site-to-site.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

El equipo de administración de sistemas de Mobbeel es el único autorizado para llevar a cabo labores de administración del entorno *cloud*. El canal de comunicación para estos mantenimientos se basa en una conexión SSHv2 segurizada con un bastión que sólo permite cifrados categorizados como recomendados en la guía CCN-STIC 807 [REF1] y eliminando la posibilidad de utilizar cifrados inseguros. Esta conexión sólo se encuentra disponible desde la red corporativa de Mobbeel. Los algoritmos configurados a nivel de servidor de Open SSH son los siguientes:

- a) **Algoritmos de cifrado:**
 - i) chacha20-poly1305@openssh.com
 - ii) aes256-gcm@openssh.com
 - iii) aes128-gcm@openssh.com
 - iv) aes256-gcm
- b) **Algoritmos de autenticación e integridad:**
 - i) hmac-sha2-512-etm@openssh.com
 - ii) hmac-sha2-256-etm@openssh.com
- c) **Algoritmos de intercambio de claves:**
 - i) curve25519-sha256@libssh.org
 - ii) ecdh-sha2-nistp521
 - iii) ecdh-sha2-nistp384
 - iv) ecdh-sha2-nistp256
 - v) diffie-hellman-group-exchange-sha256

Las labores de administración de una cuenta del módulo de agente serán llevadas a cabo por un administrador con rol de configurador. Un configurador es aquel usuario autorizado del sistema encargado de realizar cambios sobre los parámetros de configuración del sistema, siendo el único con este nivel de privilegio. A continuación, se detallan las operaciones que puede llevar a cabo.

6.3.1.1 GESTIÓN DE USUARIOS

Operaciones relacionadas con la gestión de usuarios y permisos:

- a) **Creación de un usuario:** se lleva a cabo mediante la generación de un enlace de invitación a una cuenta de correo. El configurador deberá asignar un rol al nuevo usuario y una licencia asociada. También podrá elegir si en el correo electrónico se incluye un código OTP como método 2FA.
- b) **Mantenimiento de usuarios:** para cada usuario dado de alta en el sistema el configurador podrá llevar a cabo las siguientes acciones:
 - i) **Editar usuario:** permite modificar el rol de un usuario, asignarlo a otra licencia del sistema y habilitar o deshabilitar el segundo factor de autenticación. También es posible regenerar la contraseña enviando un correo al usuario para que elija otra nueva.
 - ii) **Obtener enlace de invitación:** consultar un enlace con la invitación de registro.
 - iii) **Desbloquear usuario:** permitir de nuevo operar sin restricciones a un usuario bloqueado.
 - iv) **Regenerar enlace de invitación/confirmación:** volver a generar un enlace con la invitación de registro.
 - v) **Desactivar usuario:** eliminar temporalmente un usuario del sistema.
 - vi) **Activar usuario:** volver a permitir la operación de un usuario desactivado.
 - vii) **Eliminar:** borrar definitivamente un usuario del sistema.

6.3.1.2 GESTIÓN DE LICENCIAS Y PROPIEDADES

Operaciones relacionadas con los procesos y operativas asociadas a una licencia o cliente:

- a) Validaciones de procesos:
 - i) **Validación de procesos:** habilitar la posibilidad de que un integrador pueda añadir validaciones extra a un proceso antes de que el sistema lo marque como listo para revisión por un operador.
 - ii) **Tiempo de espera para validar un proceso:** tiempo (medido en minutos) de espera máxima para realizar validaciones sobre un proceso antes de que el sistema lo etiquete de forma automática como listo para revisión por un operador.
- b) Borrado de procesos:
 - i) **Borrado programado de procesos:** habilitar un borrado automático y programado de procesos.
 - ii) **Tiempo de gracia:** tiempo (medido en horas) que deberá pasar para borrar de forma automática un proceso si se ha habilitado previamente esta opción.
- c) Notificaciones push:
 - i) **URL de notificación:** URL a la que enviar alertas con los cambios de estado de una activación. Esta opción permite a un integrador realizar un seguimiento de los procesos activos de una manera sencilla.
 - ii) **Tiempo de reenvío de notificación push:** intervalo temporal (medido en segundos) mínimo para el envío de notificaciones sobre el cambio de estado en las activaciones.
- d) Bloqueo de usuarios:
 - i) **Tiempo de bloqueo:** tiempo (medido en horas) que deberá transcurrir para que un usuario bloqueado pueda volver a autenticarse en el sistema.

- ii) **Número de intentos máximos:** número máximo de intentos fallidos de autenticación permitidos para un usuario antes de ser bloqueado de manera automática.
- e) Revocación de contraseña:
 - i) **Días restantes para notificar:** lista con los días de antelación con los que se debe avisar a un usuario de que su contraseña está en proceso de expiración.
 - ii) **Tiempo de expiración de contraseña:** tiempo (medido en días) de vida máxima de la contraseña de un usuario. Cumplido ese valor, el usuario deberá renovar su contraseña para poder seguir operando en el sistema.
- f) Gestión de procesos:
 - i) **Tiempo máximo para aceptar un proceso entrante:** tiempo máximo (medido en segundos) establecido para que un agente pueda aceptar un proceso entrante.
 - ii) **Email de notificación:** dirección de correo electrónico a la que se notificará que un agente ha excedido el tiempo máximo establecido para el estado no disponible.
 - iii) **Enviar email agentes no disponibles:** habilitar el envío de correo electrónico al responsable cuando un agente ha excedido el tiempo máximo establecido para el estado no disponible.
 - iv) **Tiempo no disponible:** tiempo máximo (medido en minutos) establecido para que un agente puede estar en estado no disponible antes de que se envíe un email de notificación a su responsable.
 - v) **Asignación automática:** permitir el envío automático de activaciones a la cola de procesos para su revisión por un operador.
- g) Restricciones de contraseña:
 - i) **Contraseñas diferentes:** número mínimo de contraseñas diferentes permitidas antes de que pueda volver a utilizarse una anterior.
 - ii) **Longitud mínima:** tamaño mínimo (medido en caracteres) que debe cumplir una contraseña para considerarse válida.
 - iii) **Debe contener un carácter especial:** habilitar la necesidad de incluir un carácter especial en la contraseña para considerarse válida.

6.3.1.3 SEGUNDO FACTOR DE AUTENTICACIÓN (2FA)

- a) **Días para solicitar segundo factor de autenticación:** días que deben transcurrir desde el último login de un usuario para que se solicite el doble factor de autenticación a la hora de acceder de nuevo al portal del agente.
- b) **MRZ editable:** permitir la edición de la MRZ extraída del documento línea a línea para corregir posibles errores de transcripción.
- c) **OPT:** habilitar de manera general la generación de OTP para todos los procesos de autenticación.
- d) **Umbral de decisión para correspondencia facial:** valor numérico a partir del cual se considerará que las dos caras extraídas del proceso (la del selfie y la del documento) corresponden a la misma persona. El valor utilizado como referencia se establece en 50 para productos de videoidentificación que sigan los requisitos establecidos en la guía CCN-STIC 140.F11 [REF4]. El configurador puede modificarlo, tomando como referencia la gráfica que aparece a continuación (los umbrales se encuentran en el rango 0-100).

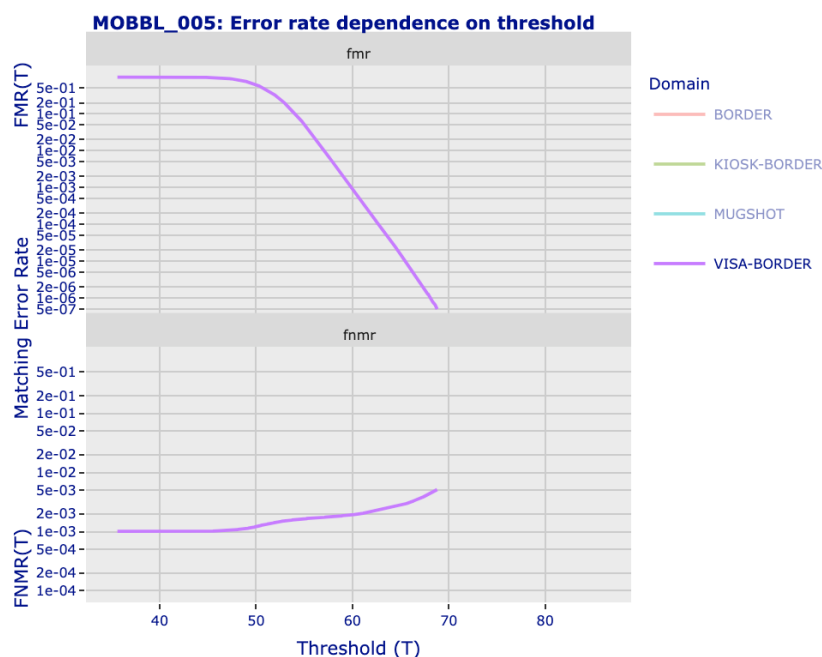


Ilustración 3. Gráfica para la configuración de umbrales de decisión biométricos

- e) **Tipo de PAD:** modalidad de prueba de vida exigida al usuario que lleva a cabo el registro como parte del sistema de detección de ataques de presentación (PAD). Incluye la eliminación de este paso (-1), la prueba de vida colaborativa (0) y la no colaborativa (2).
- f) **Umbral de decisión PAD:** valor numérico a partir del cual se considerará que no ha existido un intento de ataque de presentación al sistema biométrico. Por defecto aparece el valor 50, un umbral recomendado para la mayor parte de las aplicaciones. El configurador puede modificarlo ligeramente para hacer el sistema más seguro o accesible.
- g) **Tiempo máximo pendiente:** tiempo máximo (medido en segundos) que puede permanecer en estado pendiente una activación antes de que sea rechazada automáticamente por el sistema.
- h) **Tipo de detección de hologramas:** tipo de operativa que se solicitará al usuario que lleva a cabo el registro para comprobar la autenticidad de su documento de identidad. Incluye la eliminación de este paso (-1) y la detección de hologramas activando el flash de la cámara.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

MobbScan define dos tipos de roles de tipo administrativo (configurador y auditor) y otro de tipo operativo (operador) con las siguientes características:

- a) **Configurador:** rol administrativo con capacidad de modificar distintos parámetros de la operativa de MobbScan, como los umbrales de decisión o la gestión de usuarios. El detalle de la operativa permitida para este rol se encuentra detallado en el apartado 4 FASE PREVIA A LA INSTALACIÓN de este documento. El configurador es el único rol creado por defecto por el administrador del sistema cuando MobbScan se despliega en un nuevo entorno o aplicación. En ningún caso este rol tendrá acceso a la información privada de los procesos de videoidentificación.
- b) **Auditor:** rol administrativo con acceso a toda la información de auditoría generada por MobbScan, esto es, el detalle de eventos relacionados con la gestión de usuarios, los

procesos de videoidentificación o los cambios en la configuración. Sus acciones están descritas en el apartado 6.11 AUDITORÍA.

- c) **Operador:** rol con capacidad de revisar los procesos entrantes de videoidentificación, analizar las evidencias generadas. Sus acciones están descritas en el apartado 7.1 HERRAMIENTA DE ASISTENCIA AL OPERADOR.

Siguiendo la normativa CCN-STIC 807 [REF1] en lo relativo a requisitos de autenticación para usuarios internos en el nivel ALTO, se establece una autenticación de doble factor a través de contraseñas y OTP (vía correo electrónico). Se aplican los siguientes criterios en la política de contraseñas:

- a) Longitud mínima de contraseña 12 caracteres con un mínimo de tres tipos diferentes.
- b) Renovación obligatoria cada 3 meses.
- c) Máximo de 3 de intentos fallidos de autenticación.
- d) Prohibición de reutilizar 10 contraseñas anteriores.

Con respecto a los parámetros de sesión, un administrador configurador podrá determinar el tiempo máximo de inactividad, el tiempo mínimo de bloqueo para poder volver a autenticarse y el número máximo de intentos fallidos de autenticación antes del bloqueo.

Además, MobbScan incorpora medidas para evitar ataques de autenticación por fuerza bruta que permiten un bloqueo a tres niveles:

- a) **Bloqueo por IP:** si los intentos de autenticación no corresponden a usuarios registrados en el sistema se restringirá el acceso desde la IP (o rango de IPs) que están realizando las llamadas.
- b) **Bloqueo por usuario:** si los intentos de autenticación corresponden a usuarios registrados en el sistema.
- c) **Bloqueo por usuario e IP:** si los intentos de autenticación corresponden a usuario registrados en el sistema y además se realizan desde una misma IP.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

El cloud de MobbScan es un entorno totalmente gestionado por Mobbeel. Por ello, el integrador no debe realizar ninguna configuración de interfaces, puertos ni servicios sobre la infraestructura del cloud.

No obstante, sí existe comunicación de red entre el sistema de la organización cliente y el cloud de MobbScan. Dicha comunicación se establece a través de la SDK nativa de MobbScan (Android/iOS) integrada en la aplicación del cliente, que se conecta con los servicios del cloud mediante HTTPS sobre TLS 1.2/1.3 (puerto 443). La autenticación de las peticiones se realiza mediante un API key proporcionado por Mobbeel.

6.5 GESTIÓN DE CERTIFICADOS

El cloud de MobbScan es un entorno totalmente gestionado por Mobbeel, por lo que no es necesario que el usuario realice ningún tipo de tarea en lo relativo a la gestión de certificados. Por defecto se encuentran configurados aquellos recomendados por la guía CCN-STIC 807 [REF1]:

- a) TLS 1.3:
 - i) TLS_AKE_WITH_AES_128_GCM_SHA256
 - ii) TLS_AKE_WITH_AES_256_GCM_SHA384

- iii) TLS_AKE_WITH_CHACHA20_POLY1305_SHA256
- b) TLS 1.2:
 - i) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS 128
 - ii) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS 256

6.6 SERVIDORES DE AUTENTICACIÓN

El *cloud* de MobbScan es un entorno totalmente gestionado por Mobbeel, por lo que no es necesario que el usuario realice ningún tipo de configuración en lo relativo a los servidores de autenticación.

6.7 SINCRONIZACIÓN

El *cloud* de MobbScan es un entorno totalmente gestionado por Mobbeel, por lo que no es necesario que el usuario realice ningún tipo de configuración en lo relativo a la sincronización horaria. La configuración de servidores NTP está delegada en el prestador de servicios Amazon Web Services.

6.8 ACTUALIZACIONES

Las actualizaciones del portal del agente y el API de MobbScan se desplegarán de forma automática y transparente para el cliente, por lo que no será necesario ningún tipo de acción por su parte.

En cuanto a las SDKs nativas, Mobbeel informará de la disponibilidad de una nueva versión por correo electrónico incluyendo el detalle de los cambios y las acciones necesarias por parte del integrador en caso de que fuera necesario. Para aquellos casos donde se vea comprometida la compatibilidad (por ejemplo, modificando la estructura de una llamada) se publicará en la página de la documentación pública una guía de migración con todos los pasos a seguir.

6.9 AUTO-CHEQUEOS

El *cloud* de MobbScan se encuentra permanente monitorizado por herramientas automáticas que permiten detectar al instante cualquier incidencia como la interrupción del servicio o la lentitud inusual en las respuestas. Para ello se utiliza el servicio Amazon CloudWatch que permite establecer métricas y alarmas con acciones automatizadas en caso de problemas. Los eventos críticos o que requieran de una revisión por parte del equipo de soporte de Mobbeel serán notificados inmediatamente al canal de soporte mediante un sistema de gestión de tickets automatizado que se encargará de la gestión de la incidencia en horario 24x7.

A nivel de software, MobbScan integra Sentry para detectar y trazar posibles errores en la aplicación y comunicarlos directamente al equipo de soporte para su resolución.

6.10 ALTA DISPONIBILIDAD

El *cloud* de MobbScan se encuentra configurado en un esquema de alta disponibilidad para permitir cargas de trabajo elásticas.

Todos los servicios (tanto de primer como de segundo nivel) configuran una instancia base basada en contenedores Docker, obteniendo un Amazon Machine Instance (AMI) que se utiliza como molde para generar nuevas instancias de una manera automática. El AMI, junto con otros elementos de AWS como los grupos de auto escalado, las plantillas de lanzamiento, los *target groups* o los balanceadores de carga permiten desplegar cada servicio en un esquema elástico de alta disponibilidad y redundancia.

Esto supone que cada servicio cuenta con un número mínimo de réplicas repartidas en las distintas zonas de disponibilidad dentro de la región de AWS utilizada (Irlanda), que recibe peticiones de forma balanceada y que su número puede aumentarse o reducirse atendiendo a la demanda del servicio y tomando como referencia métricas como el uso de CPU global o memoria RAM.

En función del servicio y sus necesidades concretas se configura además el acceso a las bases de datos (RDS) o al sistema de ficheros compartidos (EFS). Ambos servicios se encuentran también desplegados en esquemas de alta disponibilidad y con creación automática de réplicas atendiendo a las necesidades de seguridad impuestas en el contexto del producto.

No es necesario que el usuario realice ningún tipo de configuración sobre el sistema de alta disponibilidad ya que se encuentra totalmente gestionado por el equipo de Mobbeel.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

A continuación, se indica la lista completa de eventos que generan un registro en el log de auditoría:

- a) Inicio de sesión de un usuario
- b) Cierre de sesión de un usuario
- c) Desbloqueo de un usuario previamente bloqueado
- d) Bloqueo de un usuario
- e) Activación de un usuario
- f) Desactivación de un usuario
- g) Modificación de una propiedad
- h) Restauración de una propiedad
- i) Comienzo de una videollamada
- j) Edición de un usuario
- k) Eliminación de un usuario
- l) Revisión de información de usuario
- m) Invitación a un usuario
- n) Regeneración de un link de registro
- o) Obtención de un link de registro
- p) Reinicio de contraseña
- q) Cambio de contraseña
- r) Revisión de eventos de usuario

- s) Borrado de eventos de usuario
- t) Borrado de eventos de proceso
- u) Registro de un usuario
- v) Confirmación de un usuario
- w) Generación del OTP
- x) Aceptación de un proceso
- y) Rechazo de un proceso
- z) Revisión de un proceso
- aa) Rechazo de revisión de un proceso

Para cada evento registrado se almacenan los siguientes datos:

- a) Identificador del proceso (UUID del proceso de videoidentificación implicado)
- b) Licencia del cliente
- c) Fecha
- d) Tipo de evento
- e) Datos particulares del evento (por ejemplo, el identificador del usuario que realiza una acción o el identificador del usuario que sufre una consecuencia).

Los logs de auditoría se encuentran centralizados y protegidos por una política de acceso condicional. Un auditor es aquel usuario autorizado del sistema encargado de revisar los registros de auditoría generados en MobbScan. Estos registros pueden haber sido generados por los usuarios autorizados del sistema (operadores, configuradores o auditores) o bien por los administradores de sistemas de Mobbeel cuando acceden al entorno de producción para llevar a cabo tareas de mantenimiento. A continuación, se detallan las funcionalidades a disposición de los auditores:

6.11.1.1 CONSULTA DE REGISTROS DE AUDITORÍA DE USUARIOS

Cuando un administrador accede con sus credenciales al portal del agente tiene la opción de visualizar los registros de auditoría de usuarios y procesos eligiendo en las pestañas de la parte superior. En el primer caso se mostrará una tabla con los registros generados por los usuarios autorizados (operadores, configuradores, auditores y administradores de sistemas) donde constan todos los detalles. Es posible utilizar los campos y desplegables de la parte superior para filtrar por diferentes criterios, de manera que sea más rápido y sencillo acceder a los registros buscados. En caso de querer eliminar uno o varios eventos puede utilizarse el icono del aspa roja de la columna Borrar o presionar el botón Borrar eventos (en este caso afectará a todos los eventos que se muestran en la tabla). Antes de proceder al borrado lógico se solicita la confirmación al auditor, mostrando un cuadro de alerta con la información que se dispone a eliminar. El propio acto de borrado generará a su vez un nuevo registro de auditoría.

6.11.1.2 CONSULTA DE REGISTRO DE AUDITORÍA DE PROCESOS

La tabla de procesos es idéntica a la de usuarios, con la única diferencia de que los eventos allí representados tienen que ver con la gestión de los procesos entrantes de videoidentificación por parte de los operadores. Un auditor podrá consultar las decisiones tomadas por los operadores sobre la validez de los procesos (incluyendo el motivo de rechazo) así como el tráfico de notificaciones push. Al igual que en el caso de los eventos de usuarios los registros pueden filtrarse y eliminarse, tanto de forma individual como en grupo.

6.11.2 ALMACENAMIENTO LOCAL

Los logs de auditoría se encuentran centralizados en una o varias instancias que agregan el contenido proveniente de los diferentes componentes de MobbScan. Un administrador con rol de auditor tendrá disponible en la parte superior del menú de navegación del portal del agente la pestaña Auditoría desde la que podrá acceder a todos los datos. También tendrá la posibilidad de borrar registros de auditoría a nivel lógico, permaneciendo no obstante de manera física en la base de datos.

Para eliminar una fila del registro de auditoría, el usuario con rol Auditor debe hacer clic en el aspa roja de la columna *Borrar*; el sistema muestra un resumen del evento y exige confirmación expresa. La eliminación es un **borrado lógico**: el registro no se destruye, se marca como eliminado y permanece almacenado y recuperable en base de datos, preservándose la integridad de la evidencia conforme a la medida op.exp.10 del ENS. La acción es deliberada y queda trazada al usuario Auditor que la ejecuta.

En aplicación del principio de segregación de funciones (op.acc.3), la capacidad de marcar registros como eliminados se restringe, mediante la política de control de acceso de la organización, al personal mínimo imprescindible con rol Auditor. Los registros se conservan durante el periodo de retención establecido, gestionándose la rotación y archivado a nivel de infraestructura por Mobbeel como operador del entorno.

6.11.3 ALMACENAMIENTO REMOTO

En el momento de redacción de este documento no se encuentra disponible la opción de enviar los logs de auditoría a una plataforma externa.

6.12 BACKUP

El *cloud* de MobbScan se encuentra respaldado por copias de seguridad periódicas siguiendo la política de continuidad de negocio y respuesta a incidentes establecida en el Sistema de Gestión de la Seguridad de la Información según la Norma ISO 27001 [REF5] implantada en Mobbeel. El usuario no necesita llevar a cabo ninguna acción de configuración ya que la gestión se encuentra delegada en el equipo de soporte y sistemas.

7 FASE DE OPERACIÓN

A continuación, se realiza un resumen de las funciones de seguridad más relevantes incluidas en MobbScan durante su operación:

- a) **Comprobación del principio de unidad de acto:** para cada proceso se almacena un UUID que permite trazar todo su ciclo de vida, además se realiza una grabación del proceso íntegro para su posterior revisión y se incluyen medidas automáticas para detectar posibles amenazas.
- b) **Verificación biométrica de identidad:** se toma una fotografía de la persona que realiza el proceso de *onboarding* para compararla con la que aparece en su documento de identidad. Además, se lleva a cabo un control automático de detección de ataques de presentación (PAD) para evitar la suplantación de identidad. También se graba un pequeño vídeo del usuario respondiendo a un desafío para asegurar que se trata de una persona real.
- c) **Verificación del documento de identidad:** se analiza el contenido del documento para detectar posibles manipulaciones. Para ello se determina la integridad de la MRZ mediante la comprobación de los dígitos de control según lo establecido en el documento ICAO 9303 [REF6], además de la coherencia entre los datos de ambas caras. También se analiza su apariencia con el fin de certificar que se trata de un documento de identidad original y no una captura a una pantalla o una impresión en papel.
- d) **Detección de ataques automatizados:** se aplican políticas de bloqueo automático multinivel cuando se detectan ataques de fuerza bruta al servicio de autenticación de usuarios.
- e) **Almacenamiento seguro de credenciales y datos sensibles:** MobbScan trabaja con una serie de activos y recursos que requieren una especial protección por su carácter crítico respecto a la seguridad de los sistemas o sensible respecto a la protección de datos personales. Para garantizar su seguridad la gestión está protegida mediante mecanismos criptológicos autorizados en la CCN-STIC-807 [REF1]. A continuación, se detallan los datos sensibles almacenados y los mecanismos de protección aplicados:
 - i) Datos de configuración: cifrado con AES256.
 - ii) Datos de auditoría: cifrado con AES256.
 - iii) Credenciales: *hashing* con PBKDF2 y cifrado con AES256.
 - iv) Datos personales: cifrado con AES256. Es de destacar que la información referente a datos personales únicamente se almacena de manera temporal hasta que un operador toma una decisión sobre la validez del proceso de videoidentificación. El almacenamiento y custodia posterior es realizado por un tercero de confianza.
 - v) Parámetros biométricos: cifrado con AES256.
 - vi) Claves criptográficas: el cifrado en reposo está delegado en los servicios RDS y EFS provistos por Amazon Web Services que cuentan con un protocolo.
- f) **Canales seguros de comunicación:** todas las comunicaciones que suponen algún intercambio con un elemento externo (como las llamadas entrantes) se llevan a cabo a través de HTTPS, con un requisito de versión mínima de TLS igual o superior a 1.2, rechazando de manera automática las conexiones con TLS 1.1 o 1.0. El conjunto de algoritmos de cifrado permitidos es el siguiente atendiendo a lo establecido en la guía CCN-STIC-807 [REF1]:
 - i) TLS_AES_128_GCM_SHA256
 - ii) TLS_AES_256_GCM_SHA384
 - iii) TLS_CHACHA20_POLY1305_SHA256

- iv) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- v) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

7.1 HERRAMIENTA DE ASISTENCIA AL OPERADOR

El portal del agente permite a un usuario operador llevar a cabo la revisión de todas las evidencias capturadas en un proceso de videoidentificación. A continuación, se describe la operativa paso a paso que debe llevar a cabo un operador para cumplir con su tarea.

7.1.1 ACCESO DEL OPERADOR AL PORTAL DEL AGENTE

Para poder acceder al portal del agente, un operador necesitará unas credenciales con las que realizar el login. Para conseguirlas, un administrador configurador deberá darle de alta en el sistema. Para ello debe hacer clic en el botón con el texto “Generar enlace de invitación” visible en la consola. A continuación, deberá incluir el correo electrónico del futuro usuario, asignarle un rol y asociarlo a una licencia del sistema. Por último, podrá decidir si enviar la invitación por correo electrónico, así como habilitar un segundo factor de autenticación (2FA). Una vez el nuevo operador reciba la notificación de invitación en su correo, podrá acceder al proceso de registro haciendo clic en el botón “Ver invitación.” Un enlace le redirigirá a una pantalla donde podrá elegir su contraseña. Esta contraseña debe cumplir con los requisitos de seguridad establecidos en el documento “Declaración de Seguridad”.

En caso de que el configurador haya optado por habilitar un segundo factor de autenticación (2FA), el nuevo operador recibirá en su cuenta de correo electrónico un código OTP que deberá introducir en la siguiente pantalla. Una vez finalizado este proceso su cuenta estará operativa y podrá acceder al portal del agente.

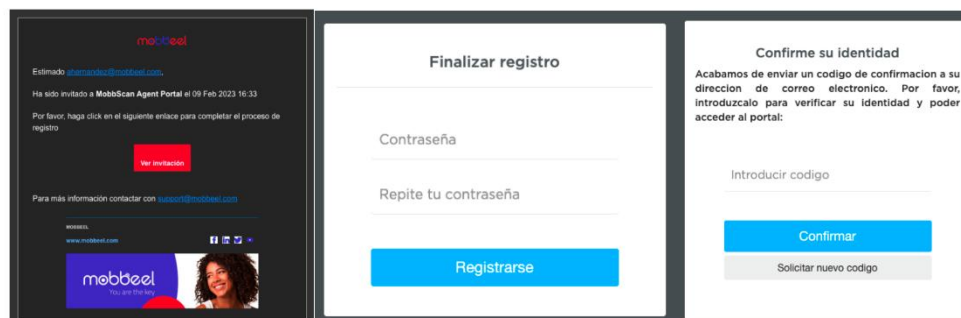


Ilustración 4. Acceso del operador

Cuando un operador accede con sus credenciales al portal del agente el sistema de asignación automática de procesos entrantes considera que está listo para comenzar a revisar activaciones. El operador se encuentra por tanto en un estado de espera.

Si es la primera vez que accede al portal o se han eliminado las preferencias de la sesión del explorador puede ser necesario habilitar las notificaciones entrantes. Cuando un proceso de activación pendiente llega al sistema éste lo asigna automáticamente a un operador disponible en función de una lógica interna que considera entre otros la carga de trabajo de cada uno de ellos. El operador puede optar entre revisar esa activación o rechazarla:

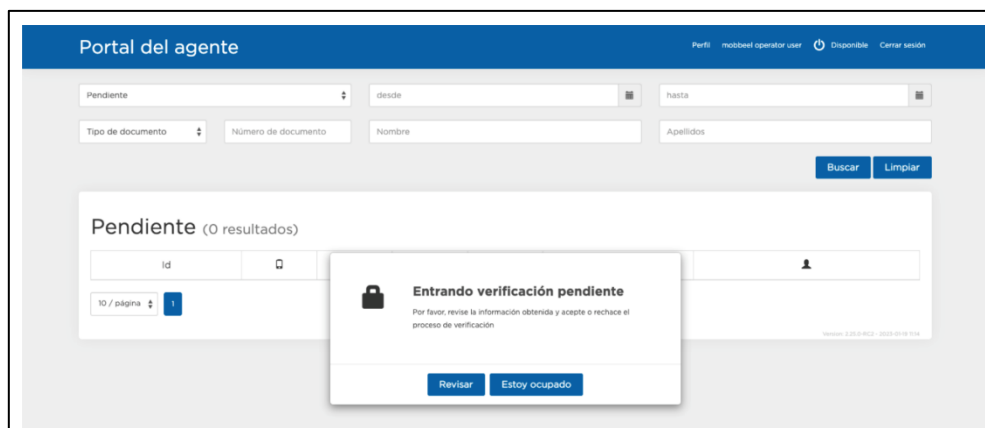


Ilustración 5. Portal del agente

En caso de optar por el rechazo (“Estoy ocupado”), el sistema colocará automáticamente al operador como no disponible y le pedirá confirmar si quiere continuar en este estado. El operador puede optar en este punto por volver a declararse como disponible (y entonces volver a recibir notificaciones) o confirmar su no disponibilidad. De forma adicional, el operador puede cambiar en cualquier momento su estado de disponible a no disponible utilizando el icono situado en la parte superior de la pantalla principal.



Ilustración 6. Cambio de disponibilidad del operador

7.1.2 REVISIÓN DE EVIDENCIAS

En el momento que el operador decide revisar una activación entrante será redirigido a la pantalla de revisión de evidencias. Esta pantalla se divide en dos regiones principales:

- a) a la izquierda se muestran los datos y validaciones obtenidos del análisis de las muestras recogidas en el proceso.
- b) a la derecha las evidencias mismas para su cotejo.

Portal del agente

Partir mobbscan operator user Cerrar sesión

🕒 Verificación pendiente

ID	182ac2a3-9740-4b21-b4f7-807b02a7e6f4
Fecha de creación	09/02/2023 10:45
Cliente	Android
OTP	338137
Movimiento al final del video	Tapar la cara con la mano

* Nombre: JUAN

* Primer apellido: ESPAÑOL

Segundo apellido: ESPAÑOL

* País: ESPAÑA

* Número personal: 65004204V

* Número de documento: AAA023112

Aceptar Rechazar Atrás

Ilustración 7. Revisión de evidencias

En la parte superior de la columna izquierda aparecen datos básicos sobre el proceso entrante:

- ID: identificador único (UUID) que permite trazar de manera unívoca el ciclo de vida de una activación.
- Fecha de creación: fecha y hora de comienzo del ciclo de vida de una activación.
- Cliente: plataforma de origen de la activación.
- OTP: secuencia aleatoria de números mostrada al usuario y que éste ha tenido que repetir durante el proceso de videoidentificación. El operador deberá cotejar con la evidencia del vídeo que el OTP ha sido pronunciado de manera correcta.
- Movimiento al final del vídeo: gesto pedido al usuario al final del proceso de videoidentificación como elemento adicional de detección de vida. El operador deberá cotejar con la evidencia del vídeo que el usuario lo ha ejecutado según lo esperado.

Debajo de los datos básicos del proceso aparecen los campos donde se muestra la información personal extraída del documento. La mayoría de estos campos son editables y el operador deberá cotejar con la imagen del documento si la transcripción es correcta, corrigiéndolos en caso contrario. A continuación, se listan los datos extraídos (dependiendo del tipo de documento algunos de ellos pueden no estar disponibles):

- Datos personales del documento: nombre, primer apellido, segundo apellido, país de emisión del documento, número personal, número de documento, fecha de nacimiento, fecha de expiración, país de nacimiento, ciudad de nacimiento, provincia de nacimiento.
- MRZ: se trata de la zona de lectura mecánica del documento de identidad. Recoge los datos personales básicos y una serie de dígitos de control que permiten validar su contenido. Si el configurador ha determinado que la MRZ puede ser modificable se dará la opción al operador de realizar cambios en la misma, en caso contrario aparecerá bloqueada.

7.1.2.1 VALIDACIONES

El área de validaciones permite al operador comprobar de manera rápida si existen elementos de sospecha sobre la validez de un proceso entrante. Estas validaciones pueden

afectar al contenido de los datos personales, a las comprobaciones biométricas o a la apariencia del propio documento. El operador deberá cotejar con las evidencias las validaciones marcadas como sospechosas (marca naranja) para tomar una decisión sobre la validez del proceso.

Las validaciones proceden de análisis automáticos de la herramienta y no tienen por qué llevar de manera directa al rechazo de una activación. Su objetivo único es servir de ayuda al operador en la toma de decisión. Los criterios de aparición de marcas verdes (resultado positivo del análisis automático) o naranjas (resultado negativo del análisis automático) están relacionados con el uso de umbrales de decisión. Por defecto estos valores están ajustados en el 50%, es decir, valores superiores al 50% significarán aceptación y viceversa. Los elementos a validar son los siguientes:

- a) MRZ: la MRZ tienen el formato esperado y todos los dígitos de control se han validado de manera correcta.
- b) Documento en vigor: la fecha de expiración es superior a la fecha actual.
- c) Mayor de edad: la diferencia entre la fecha actual y la fecha de nacimiento es de al menos 18 años.
- d) Mismo nombre en las dos caras: el nombre que consta en la MRZ y el anverso del documento es el mismo.
- e) Mismo apellido en las dos caras: el apellido que consta en la MRZ y el anverso del documento es el mismo.
- f) Mismo número de documento en ambas caras: el número de documento que consta en la MRZ y el anverso del documento es el mismo.
- g) Apariencia frontal: la apariencia del anverso del documento corresponde con la de un documento válido: no es una fotocopia, el contorno no presenta cortes, etc.
- h) Apariencia trasera: la apariencia del reverso del documento corresponde con la de un documento válido: no es una fotocopia, el contorno no presenta cortes, la fuente de la MRZ coincide con la esperada, etc.
- i) Elementos dinámicos de seguridad: el kinegrama del documento de identidad corresponde con el de un documento válido. Se analiza además la presencia de elementos anómalos, como una fotografía facial superpuesta a la original del documento.

En último lugar (y sólo para los documentos que incluyen una dirección postal), se da la opción al operador de modificar la dirección extraída por el OCR en caso de que existan inconsistencias o el usuario haya cambiado de residencia.

En la columna derecha aparecen todas las evidencias recogidas en el proceso, esto es:

- a) Vídeo completo del proceso de videoidentificación.
- b) Imagen del anverso del documento.
- c) Imagen del reverso del documento.
- d) Comparación biométrica entre la imagen del documento y la tomada al usuario durante el proceso de videoidentificación.
- e) Resultado del proceso de detección de ataques de presentación.
- f) Resultado del proceso de verificación de elementos dinámicos de seguridad.

Una vez analizadas todas las evidencias recogidas en el proceso de videoidentificación el operador deberá tomar una decisión sobre la validez de la activación. Los criterios que regirán esta decisión dependerán de las necesidades de cada caso particular, por lo que el operador deberá seguir el protocolo marcado. En caso de aceptar la activación terminaría

el proceso y el operador retornará a la pantalla de espera hasta que aparezca otra notificación.



Ilustración 8. Interfaz de Aceptación/Rechazo

En caso de rechazarla deberá indicar el motivo de la decisión escogiendo uno de los que aparecen en el desplegable. Una vez marcado y confirmado, retornará a la pantalla de espera:



Ilustración 9. Interfaz de razón de rechazo

7.2 MANTENIMIENTO

El *cloud* de MobbScan se encuentra mantenido por Mobbeel de manera que las tareas de mantenimiento durante la operación se reducen a las de carácter interno al servicio, delegando todas aquellas relacionadas con la administración de la arquitectura o la seguridad. El cliente deberá llevar a cabo las siguientes operaciones de manera periódica:

- Estar pendiente de posibles actualizaciones de las SDKs nativas y actualizar cuando corresponda siguiendo las indicaciones del equipo de soporte y de las guías de migración.
- Inspección y mantenimiento de los logs de auditoría para comprobar mediante muestreo el buen funcionamiento del sistema y de los usuarios implicados en las operaciones. Sólo los administradores con rol de auditor podrán tener acceso a los mismos.
- Gestionar los usuarios de una licencia. El administrador configurador podrá crear o eliminar nuevos perfiles, así como modificar los permisos asociados a los mismos. Se recomienda la implantación del principio de mínimo privilegio.
- Los operadores deberán ejercer su labor de revisión de los procesos de videoidentificación y tomar decisiones sobre la validez de estos apoyándose en los controles automáticos ofrecidos por MobbScan.
- En caso de incidencia en el servicio, el cliente podrá contactar con el equipo de soporte 24x7 de Mobbeel. Un sistema de gestión automatizado de incidencias se encargará de la gestión del ticket siguiendo el protocolo de escalado establecido.

8 REFERENCIAS

- [REF1] Guía de Seguridad de las TIC CCN-STIC 807
<https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html>
- [REF2] Documentación pública de SDK nativa Android
https://developers.mobbeel.com/docs/mobbscan-android/mobbscan-android_configure_sdk.html
- [REF3] Documentación pública de SDK nativa iOS
https://developers.mobbeel.com/docs/mobbscan-ios/mobbscan-ios_configure_sdk.html
- [REF4] Taxonomía de productos STIC. Anexo F.11: Herramientas de Videoidentificación
<https://www.ccn-cert.cni.es/en/series-ccn-stic/guias-de-acceso-publico-ccn-stic/5461-guia-140-anexo-f-11-herramientas-de-videoidentificacion/file.html>
- [REF5] UNE-ISO/IEC 27001:2023
<https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0071320>
- [REF6] ICAO 9303. Machine Readable Travel Documents
https://www.icao.int/sites/default/files/publications/DocSeries/9303_p1_cons_es.pdf
- [REF7] 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

2FA	<i>Two Factor Authentication</i>
AMI	<i>Amazon Machine Instance</i>
API	<i>Application Programming Interface</i>
AWS	<i>Amazon Web Services</i>
ENS	<i>Esquema Nacional de Seguridad</i>
HTTPS	<i>Hypertext Transfer Protocol Secure</i>
ICAO	<i>International Civil Aviation Organization</i>
MRZ	<i>Machine Readable Zone</i>
NTP	<i>Network Time Protocol</i>
OTP	<i>One Time Password</i>
PAD	<i>Presentation Attack Detection</i>
SDK	<i>Software Development Kit</i>
SSH	<i>Secure Shell</i>
TLS	<i>Transport Layer Security</i>
TSP	<i>Trust Service Provider</i>

