4DIGITAL AI TECHNOLOGIES

AI OPERATIONAL INTELLIGENCE

AOI
Identity

Identidad, evidencia y contexto para su operación de seguridad.



MINERÍA Y GRANDES OPERACIONES INDUSTRIALES

Reconocimiento facial, gestión de identidades y observaciones trazables para apoyar a los equipos de seguridad en puntos definidos de la operación.

01 / IDENTIDAD CON EVIDENCIA OPERACIONAL

Ayude a su equipo a responder quién fue observado y dónde.

AOI Identity relaciona reconocimiento facial, galerías y evidencia visual con cámaras, ubicaciones y referencias temporales definidas.

01 Agilice la revisión de observaciones

Reúna las coincidencias propuestas y su evidencia para que el equipo autorizado pueda revisar cada situación con contexto.

02 Mantenga una base de identidad gobernada

Organice candidaturas, revisión y publicación de galerías. Distinga una identidad aprobada de su activación confirmada en el equipo de destino.

03 Conecte la identidad con la operación

Consulte observaciones y contraste la información disponible con fuentes de acreditación, respetando las reglas y responsabilidades del cliente.

Dos experiencias que se complementan

Identity / administración

Gestión biométrica, candidaturas, galerías y sincronización.

Security / operación

Últimas observaciones, búsqueda de personas, cámaras, eventos y evidencia.

02 / DE LA CANDIDATURA A LA ACTIVACIÓN

Cada identidad avanza con estados verificables.

El flujo definido conserva la revisión humana y permite distinguir la publicación de una galería de su disponibilidad efectiva en AICE.

01

Candidatura

Evidencia disponible para proponer una identidad.

02

Revisión

Evaluación y aprobación por el rol autorizado.

03

Publicación

Envío de la identidad o galería aprobada al destino.

04

Activación confirmada

Confirmación de disponibilidad en el equipo receptor.

Una publicación pendiente de confirmación conserva ese estado hasta recibir la respuesta del destino.

Galerías con contexto

La configuración determina qué identidades se distribuyen a cada destino autorizado.

Sincronización visible

El seguimiento permite revisar estados de envío y confirmación dentro del alcance habilitado.

Evidencia para revisar

Las candidaturas se evalúan junto a sus imágenes y antecedentes disponibles.

03 / UNA VISTA PARA EL EQUIPO DE SEGURIDAD

Revise la observación. Acceda a su evidencia.

Security concentra la consulta operacional. Identity conserva la administración biométrica y de galerías.

AOI / SECURITY VISTA CONCEPTUAL



ÚLTIMA OBSERVACIÓN

PUNTO

Acceso A-01

HORA

09:42:18

IDENTIDAD CANDIDATA

DEMO-014

Coincidencia por revisar

Cámara C-01 / Evidencia de la observación seleccionada

Interfaz conceptual con persona, identificación y registro ficticios.

01

Consultar

Últimas observaciones y búsqueda de personas dentro de las fuentes autorizadas.

02

Investigar

Cámara, ubicación, hora y evidencia para revisar cada episodio.

03

Verificar fuentes

Estado de las cámaras y vigencia de los datos que acompañan la consulta.

La última observación indica un punto y un momento; no acredita la ubicación actual de una persona.

04 / INFORMACIÓN DISTINTA, CONTEXTO COMPARTIDO

Relacione identidad y acreditación con criterios claros.

La integración permite contrastar la observación con registros del cliente. Cada fuente mantiene su función dentro de la decisión operacional.

DIMENSIÓN	PREGUNTA	FUENTE O CRITERIO
Identidad	¿Con qué identidad puede corresponder la observación?	Reconocimiento facial, galería y revisión disponible.
Acreditación	¿Qué condición registra la fuente del cliente?	Sistema de acreditación y fecha de actualización.
Autorización	¿Corresponde permitir el acceso en este contexto?	Reglas, vigencias y sistema responsable definidos por el cliente.

Sincronización con la fuente del cliente

La lectura de la base de acreditación se configura con una periodicidad acordada. La consulta debe conservar la referencia de actualización para interpretar qué información estaba disponible en cada momento.

Una coincidencia facial no concede acceso por sí sola. Las acciones sobre puertas o controles requieren integración y reglas expresamente definidas.

05 / PUNTOS DE OBSERVACIÓN DEFINIDOS

Visibilidad de identidad en espacios operacionales.

La cobertura se diseña a partir de los flujos peatonales y de las necesidades de Seguridad Patrimonial y de la operación.



Escena conceptual. Persona e instalación ficticias.

CAMPAMENTOS Y RECINTOS

Revisar observaciones en accesos y corredores definidos, con evidencia por punto y horario.

ACCESOS A ÁREAS INDUSTRIALES

Contrastar observaciones con la información de identidad y acreditación disponible para el área.

CENTROS OPERACIONALES

Facilitar la consulta de eventos e identidades por el personal autorizado desde la vista Security.

INSTALACIONES CON VARIOS PUNTOS

Organizar cámaras y destinos de galerías, manteniendo trazabilidad de las observaciones y la sincronización.

El alcance se acuerda por puntos, cámaras, galerías y fuentes. Cada nuevo emplazamiento requiere revisar cobertura y condiciones de captura.

06 / AICE Y AOI CON FUNCIONES COMPLEMENTARIAS

Procesamiento en el borde. Gestión y revisión en AOI.

Identity se incorpora al ecosistema existente de AICE y AOI, conservando las funciones y servicios de cada plataforma.



La activación se confirma desde el destino. La publicación conserva su estado hasta recibir esa confirmación.

AICE Identity — Interfaz específica para el módulo y su operación local, junto a los servicios existentes.

AOI Identity — Candidaturas, revisión, galerías y seguimiento de sincronización dentro del módulo.

Security — Experiencia operacional para consultar personas, observaciones, cámaras y eventos.

07 / CALIDAD DE CAPTURA Y USO RESPONSABLE

La confianza comienza en cada punto de observación.

El desempeño se valida en el entorno real: ubicación, iluminación, movimiento, visibilidad facial y calidad de la evidencia.



Imagen conceptual de una persona ficticia.

INGENIERÍA DE CAPTURA

- Encuadre y distancia adecuados
- Iluminación y exposición
- Nitidez y visibilidad facial
- Pruebas en sentidos de circulación
- Verificación de calidad por cámara

Validación biométrica

Ajustar criterios de coincidencia y evaluar falsas coincidencias, omisiones y evidencia insuficiente por punto.

Galerías y permisos

Definir usuarios, destinos autorizados, retención y responsabilidades de revisión según las políticas del cliente.

Pruebas de suplantación

Validar el comportamiento frente a fotografías y pantallas. Su estado de aceptación se documenta dentro del proyecto.

Una observación sin coincidencia suficiente se conserva como tal y requiere el tratamiento definido por la operación.

08 / ADOPCIÓN CON CRITERIOS VERIFICABLES

Comience con puntos clave. Valide antes de ampliar.

Operaciones, Seguridad Patrimonial y TI definen el alcance junto con el equipo de implementación.

01	**Definir los puntos**	Acordar flujos, ubicaciones, cámaras y finalidad de la consulta.
02	**Preparar las fuentes**	Habilitar conectividad, encuadres y acceso a los registros autorizados.
03	**Configurar identidades**	Establecer candidaturas, revisión, galerías y destinos de publicación.
04	**Integrar y sincronizar**	Conectar las fuentes y verificar la activación en cada equipo receptor.
05	**Validar en terreno**	Contrastar calidad de observación, coincidencias y pruebas acordadas.
06	**Operar y ampliar**	Capacitar, definir soporte y extender los puntos que cumplen los criterios.

CÓMO EVALUAR EL VALOR

Calidad de evidencia y eficiencia de revisión

Mida tiempo de consulta, proporción de observaciones revisables, errores de coincidencia y estado de sincronización. Acuerde referencias y metas por punto de observación.



AOI IDENTITY

Conecte identidad, evidencia y contexto en su operación.

Diseñemos la visibilidad que su equipo necesita.

Con Seguridad Patrimonial, Operaciones y TI, seleccionamos los puntos prioritarios, revisamos las fuentes y definimos una implementación con criterios de aceptación.

Conozca AOI y coordine una demostración

4digital.ai

ALCANCE Y DISPONIBILIDAD

Las vistas, funciones biométricas, galerías e integraciones se acuerdan por versión y proyecto. El desempeño y las pruebas de suplantación requieren validación en cada entorno. La acreditación y la autorización conservan sus reglas y fuentes responsables.

Imágenes e interfaces conceptuales con personas y datos ficticios. No representan una instalación ni resultados de un cliente.