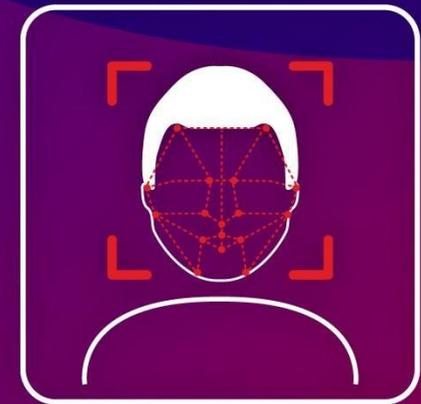




# Face Recognition 2.0

Nuevo enfoque en el reconocimiento facial  
módulo de análisis de vídeo TRASSIR para  
reconocimiento facial





La marca TRASSIR fue creada para llevar al mercado sistemas de CCTV de alta tecnología. La marca combina de equipos profesionales de procesamiento de video (cámaras, servidores, módulos de análisis) y software basado en redes neuronales. Los módulos de análisis de TRASSIR se utilizan para monitorear y proporcionar acceso, monitoreo perimetral, delimitación de áreas peligrosas y monitoreo del uso de ropa protectora.

La función principal del equipo es garantizar la seguridad de los clientes y mejorar la eficiencia de su negocio. Se desarrollaron y patentaron tecnologías innovadoras bajo la marca TRASSIR: servidor de video IP, grabadores de video y NVR más, cámaras IP patentadas emblemáticas.

# 20 AÑOS

Experiencia en videovigilancia

# 5000+

Clientes por todo el planeta

# 800+

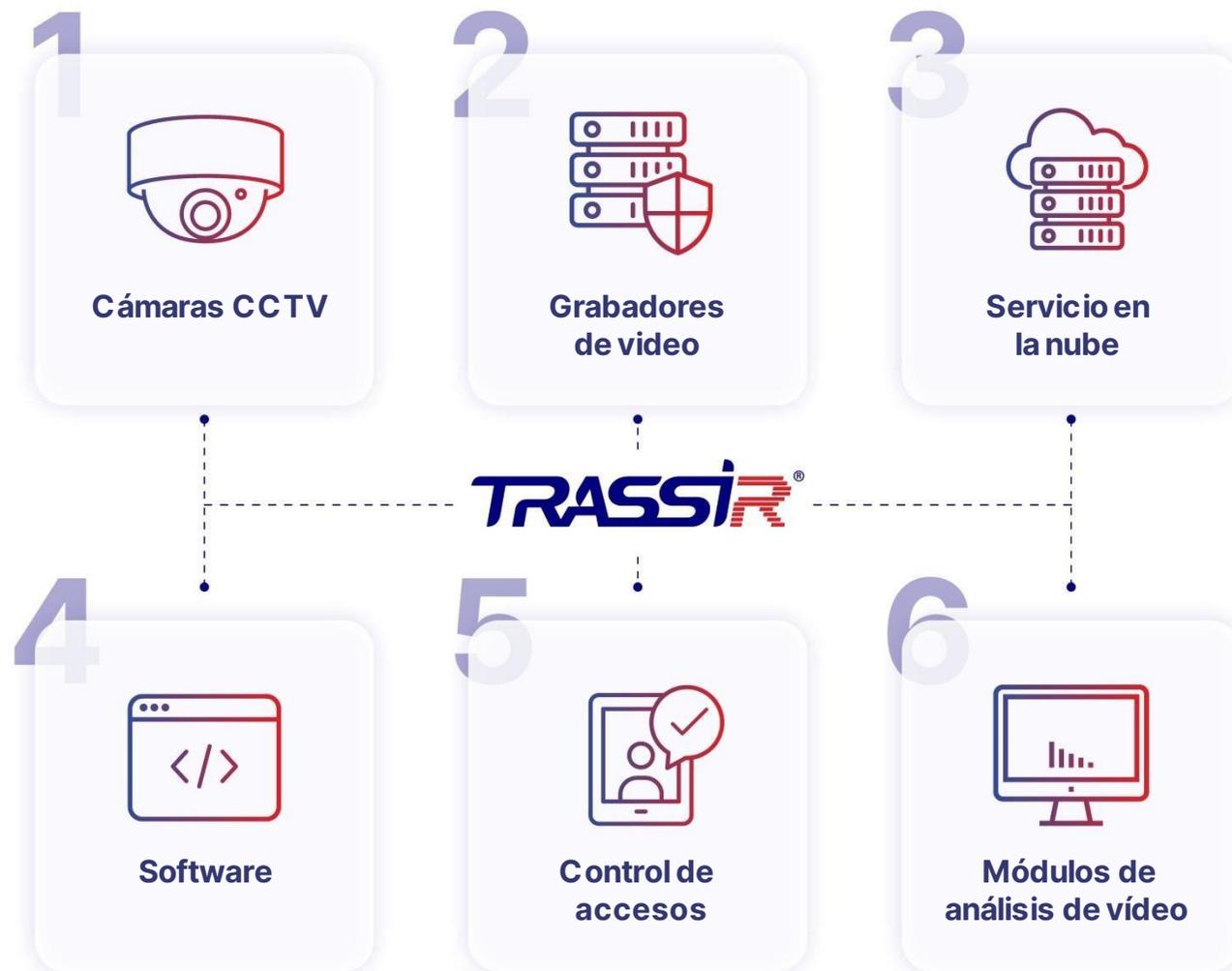
Empleados cualificados

# 35 PAISES

Con soluciones integradas TRASSIR



**TRASSIR**  
ecosistema  
para una  
supervisión eficaz  
de la seguridad



**TRASSRFace Recognition 2.0 –  
una nueva versión mejorada del módulo de  
análisis de vídeo inteligente Face  
Recognition para el reconocimiento facial y  
la búsqueda de personas basada en una  
base de datos preconfigurada.**

Demuestra alta eficiencia,  
confiabilidad y reconocimiento  
correcto en una amplia gama de  
escenarios.

Face Recognition



Face Recognition 2.0

**El principio de funcionamiento del  
módulo: crear una base de datos de  
rostros y verificar cada rostro detectado en  
tiempo real para determinar la coincidencia  
con alguna persona en la base de datos.**

- Calidad de detección de rostros – 99.8%
- Funciona tanto como parte de un solo servidor como en un sistema multiservidor con una base de datos de una sola persona
- Incluye la opción de copiar y sincronizar la base de datos de rostros
- Permite importar una base de datos con fotos para reconocimiento y búsqueda



## Face Recognition 2.0

### Características del módulo



## CAPACIDAD PARA RECONOCER EL USO DE UNA FOTO EN UN MARCO, DETERMINANDO LA MITACIÓN "EN VIVO" DE UNA CARA

Funciona en base a la tecnología de detección pasiva, que es adecuada para el control de acceso: puede distinguir a una persona del uso de una foto para engañar.

La red neuronal analiza los fotogramas y captura los cambios en la cara, comparándola con una imagen estática.



### VENTAJAS:

- ✓ No requiere interacción de la cara que se detecta con el sistema
- ✓ El módulo es compatible con cualquier equipo existente
- ✓ Requiere menos recursos que la versión anterior

## BÚSQUEDA DE PERSONAS EN FUNCIÓN DE DETERMINADOS ATRIBUTOS DE APARENCIA

Permite obtener atributos faciales para análisis avanzados y búsqueda de personas en función de parámetros dados (raza, edad, sexo, color de pelo, barba, bigote, gafas, sombreros, máscara protectora).

Uso de la base de datos de un servidor TRASSIR local o remoto con la opción de copiar, importar y sincronizar la base de datos externas.

## CREACIÓN DE UNA BASE DE DATOS DE PERSONAS ÚNICAS

The database of unique persons stores reference photos with which a comparison is made. All appearances of the recognised person in the video are viewed in the face log.

### Cómo se ejecuta el filtrado

La búsqueda de un intruso mediante filtros de atributos es ultrarrápida. Puede trazar la ruta de movimiento e identificar posibles cómplices. Características del filtro: sexo, edad, raza, vello facial, sombreros, gafas, emociones, color de cabello, máscara.

1

### Cómo se crea la base de datos de rostros únicos

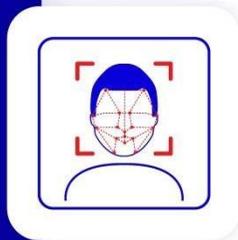
La apariencia del mismo rostro una imagen de video se ingresa automáticamente en la 'Persona' como una carpeta en una computadora. La 'Persona' acelera y simplifica la búsqueda en un gran archivo de video y en transmisiones de video en tiempo real desde cámaras de CCTV.

2

## USING A CENTRAL FACE DATABASE

### Compatibilidad con sistemas multiservidor

Face Recognition 2.0 soporta un sistema multiservidor: funciona con un único servidor como en un sistema multiservidor con una única base de datos de rostros, optimizando así recursos del servidor.



### Sincronización de bases de datos

Permite copiar y sincronizar la base de datos, lo cual es crucial para un funcionamiento eficiente con un canal de comunicación inestable.

# CONTEO DE VISITANTES ÚNICOS

La función de análisis de visitantes funciona integrando al módulo TRASSIR Face Recognition 2.0 el módulo TRASSIR Face Analytics, un módulo de reconocimiento facial y análisis.

## Conteo visitantes únicos

**TRASSIRFace Recognition 2.0** reconoce a los visitantes únicos y permite configurar contadores faciales en cámaras conectadas. Determina el número de personas en la imagen con un alto grado de precisión.

### Ventajas:

La función de conteo de visitantes es necesaria para monitorear colas y áreas de espera, espacios públicos y prevenir reuniones sospechosas no autorizadas.

## Análisis de visitantes

**TRASSIRFace Analytics** analiza los datos y recopila estadísticas sobre el sexo, la edad, el número de visitantes únicos y recurrentes. Mejora la calidad del servicio y ofrece bienes y servicios realmente necesarios.

### Ventajas:

La recopilación y el análisis de datos cuantitativos precisos sobre los visitantes en instalaciones y eventos mejoran la seguridad y la organización de eventos.

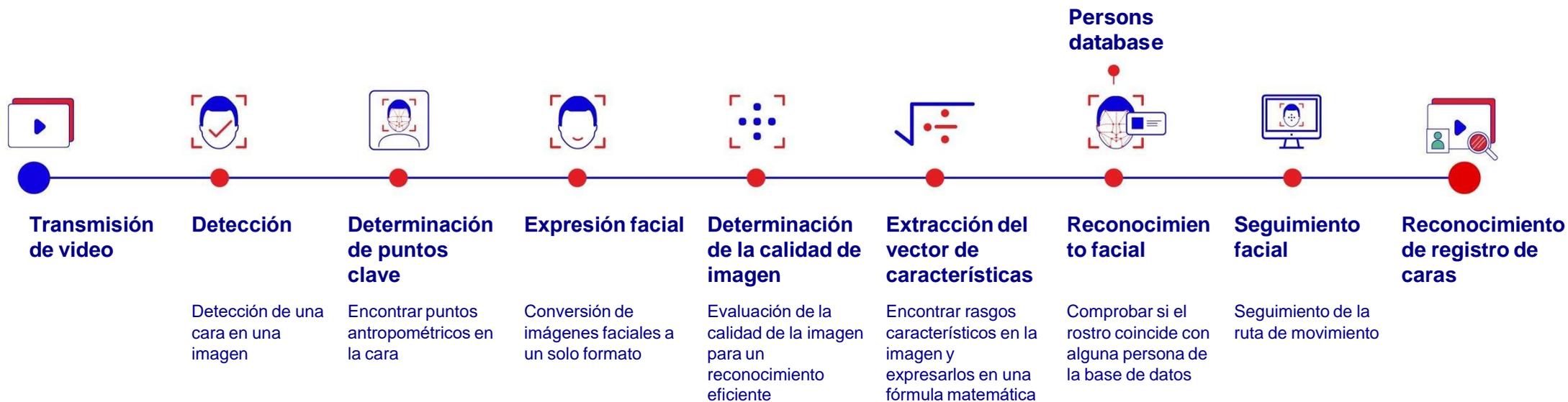


## Face Recognition 2.0

### Características del módulo

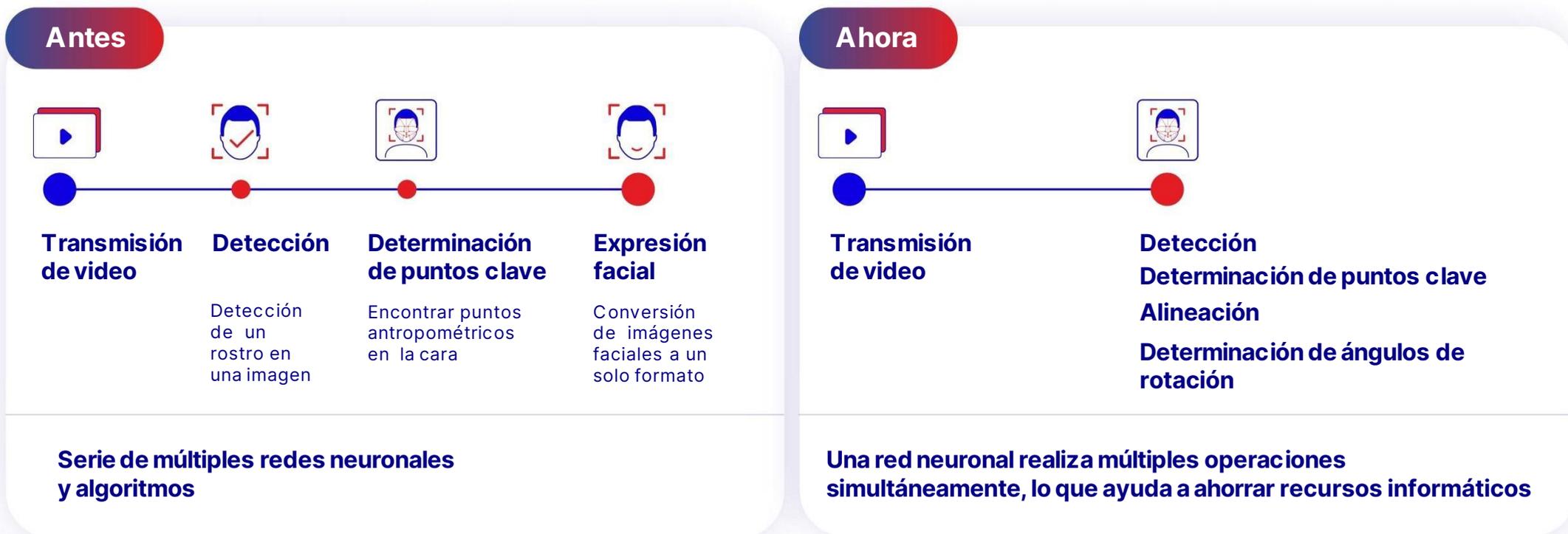


# ¿CÓMO FUNCIONA EL RECONOCIMIENTO FACIAL?



# FUNCION ACTUALIZADA: ARQUITECTURA ÚNICA

Desarrollamos una arquitectura única que permite realizar simultáneamente múltiples etapas en el reconocimiento facial.



# FUNCIONALIDAD ACTUALIZADA: TECNOLOGÍA DE FILTRADO DE DETECCIÓN FALSA

Implementamos una nueva tecnología de filtrado de detección de falsos basada en clustering.

## Principio de funcionamiento

### Las caras se distribuyen en grupos por similitud

→ La red neuronal distribuye condicionalmente los rostros en 400.000 clústeres agrupados por su similitud y determina la similitud a un clúster específico

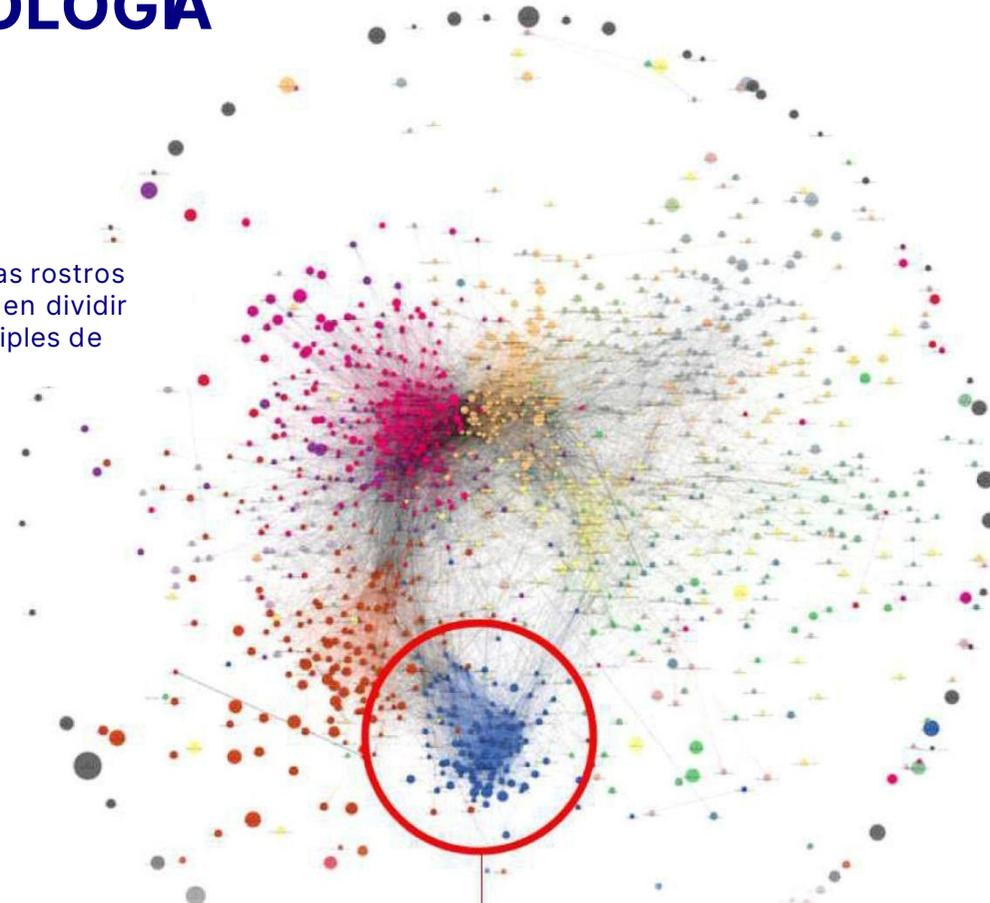
### Se forma un 'cúmulo de basura'

→ El clúster 'basura' incluye imágenes de baja calidad de rostros e imágenes de objetos que no son rostros

### La detección falsa se identifica y se descarta

→ Después de resaltar los rasgos faciales, se comprueba si corresponde en el 'grupo de basura'. Si es así, lo más probable es que sea una detección falsa y se descarte.

Todos los rostros se pueden dividir en múltiples de grupos



Si un rostro se registra en este grupo, ¡lo más probable es que sea una detección falsa!

## FUNCIONALIDAD ACTUALIZADAS: MECANISMO DE SEGUIMIENTO FACIAL DE ALTA PRECISIÓN

Introducimos un nuevo mecanismo de seguimiento facial.

### Antes: seguimiento óptico

- Baja eficiencia cuando Los rostros se superponen entre sí
- Baja eficiencia con un mal ángulo

### Ahora: seguimiento basado en vectores de características

- Si una cara desapareció del marco y luego reapareció, un nuevo rastreador la empareja con una pista detectada previamente, comparando rasgos faciales únicos



## COMPARACIÓN DE INDICADORES

### Calidad de detección de rostros:

- Versión antigua 88%
- Nueva versión 99.8%

### Calidad del reconocimiento:

- En ángulos difíciles, la nueva versión reconoce con un 20% de mayor precisión

### Número de reconocimientos faciales falsos:

- Versión antigua 11
- Nueva versión ~0%

### Número de detecciones falsas:

- El número de detecciones de rostros falsos (brazos, piernas, bolsas, etc.) cae a 0



**Soluciones  
empresariales  
y de seguridad listas  
para usar con  
Face recognition 2.0**



## SECTOR BANCARIO

### → Detección de documentos falsificados

Si existe la sospecha de que el cliente presentó un contrato falso a otra persona para realizar un retiro, el gerente compara la foto del verdadero propietario del acuerdo de la base de datos del sistema con el posible estafador. Toma medidas si se confirma el fraude.

### → Detección del robo de tarjetas bancarias

Un cliente olvidó la tarjeta en el cajero automático, el siguiente cliente la sacó antes de que el cajero automático la retuviera e hiciera compras. El incidente fue investigado: el rostro del ladrón fue reconocido y puesto en la lista negra.

### → Impedir transacciones con la tarjeta bancaria de otra persona

El sistema reconoce la cara de la persona que realiza la transacción con la tarjeta en el cajero automático y la compara con la foto del verdadero propietario de la tarjeta. Si hay una discrepancia, el administrador se pone en contacto con el verdadero propietario o bloquea la tarjeta.

### → Evitar el acceso no autorizado a los datos

Un sistema de control de accesos con doble autorización basado en características biométricas ayudará a evitar que un intruso entre en la oficina bancaria y filtre información: se evita el uso de un pase robado o del pase de otra persona en complicidad con el propietario. La cara del ladrón es reconocida y puesta en la lista negra.

## RETAIL

### → Lucha contra hurtos

Al detectar el robo, la cara del ladrón se reconoce y se registra en una sola "lista negra". Si el ladrón regresa, se le prohíbe la entrada o sus acciones son monitoreadas cuidadosamente.

### → Lucha contra el fraude de los empleados

El reconocimiento facial detecta la asistencia de los empleados, detecta a los 'trabajadores fantasmas' empleados para que otra persona reciba su salario y evita el fraude con las horas de trabajo mediante el uso de pases de otras personas.



## INDUSTRIA

### → **Prevención del robo, vandalismo, terrorismo**

El personal de seguridad de grandes empresas no puede recordar físicamente todas las caras de los empleados y trabajadores contratados. Por lo tanto, alguien podría ingresar al sitio usando un pase falso. Un sistema de control de acceso integrado con módulos de reconocimiento facial identifica y evita el pase de intrusos.

### → **Mantenimiento de la privacidad**

Un sistema de control de acceso con autorización basada en identificadores y rostros, utilizando un módulo de reconocimiento facial, evita el acceso no autorizado como resultado del robo de identificadores o su transferencia a terceros.

### → **Seguimiento de las visitas a la empresa**

Un sistema de control de acceso se engaña presentando un identificador y una fotografía grande de su propietario en el puesto de control en lugar de la persona real para simular la llegada de la persona al lugar de trabajo, ocultando el ausentismo. La tecnología de reconocimiento de 'vitalidad' facial detectará el fraude de pases.



## CENTROS DE NEGOCIOS Y OFICINAS

### ➔ Monitoreo del desempeño de los empleados

El sistema de control de acceso, integrado con el módulo de reconocimiento facial, determina la hora de llegada y salida del empleado, las horas reales de trabajo, el tiempo pasado en la sala de fumadores, moviéndose entre habitaciones y genera automáticamente un informe para tomar medidas.



## RESTAURANTES Y HOTELES

### → Promoción de marca en Internet, evaluación de la efectividad de la publicidad

Face Recognition 2.0 reconoce a los visitantes únicos y recurrentes, realiza análisis demográficos y calcula la conversión. Los análisis realizados mejoran la efectividad de la publicidad dirigida, después de lo cual Face Recognition 2.0 calcula la afluencia de nuevos visitantes únicos.

### → Monitoreo del desempeño de los empleados

El personal de seguridad de los grandes restaurantes no puede recordar los rostros de un gran número de empleados y reconocer a una persona que viola la disciplina en el lugar de trabajo. Face Recognition 2.0 reconoce a los infractores, genera automáticamente un informe sobre las horas de trabajo reales y el tiempo pasado fuera del lugar de trabajo, que se convertirá en la base de sanciones o amonestaciones..

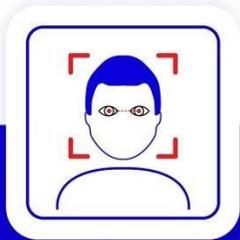


**TRASSIR®**

**Recomendaciones sobre  
la elección de cámaras y  
grabadores de video**



## SELECCIÓN DE CÁMARAS



Para el correcto funcionamiento del detector, la distancia entre las pupilas de la imagen resultante debe ser de al menos 60 px.

La distancia media entre las pupilas de un adulto es de 64 mm. Por lo tanto, la densidad de píxeles en el área de captura debe ser  $60/64 \sim 0.938 \text{ px/mm}$   
 $= 938 \text{ px/m}$ .



### La resolución de cámara requerida depende del ancho del campo de visión:

- ✓ Con una distancia al objeto de 5 metros y una amplitud del campo de visión de 2 metros, la resolución requerida es de 2MP

---

- ✓ Con una amplitud de 3 metros – 5MP

---

- ✓ Con una amplitud de 4 metros – 8MP

# CÁMARAS TRASSIR PARA EL MÓDULO DE RECONOCIMIENTO FACIAL 2.0

## SISTEMA DE CONTROL DE ACCESOS EN OFICINAS



### TR-D2D2 v2

- 2MP resolución
- Matriz 1/2.9, sensibilidad 0.003lx
- En interiores

## INGRESO A TIENDAS



### TR-D4151IR1

- 5MP resolución
- Matriz 1/2.8, sensibilidad 0.003lx
- Carcasa que no llama la atención

## INGRESOS A RESTAURANTE



### TR-D8181R3 v2

- 8MP resolución
- Matriz 1/2.7, sensibilidad 0.005lx
- Carcasa adecuada tanto para uso en interiores como en exteriores

## GRABADORES DE VIDEOTRASSIR PARA EL MÓDULO DE RECONOCIMIENTO FACIAL 2.0



### NeuroStation Compact RE

Grabador de red de bajo costo para cámaras IP que funcionan en TRASSIR OS (Linux) con soporte de análisis de video

Número de canales disponibles para el módulo Face Recognition 2.0: hasta 10 canales



### NeuroStation

La mejor opción para una grabadora de video de red en términos de relación calidad-precio y soporte de análisis de video

Número de canales disponibles para el módulo Face Recognition 2.0: hasta 26 canales



### UltraStation - I

Grabadores de vídeo de alta capacidad con almacenamiento de datos fiable hasta 465,66 TB

Número de canales disponibles para el módulo Face Recognition 2.0: hasta 13 canales



¡Gracias por su atención!



 [trassir.com](https://trassir.com)

 [welcome@trassir.com](mailto:welcome@trassir.com)