



ID-GATE

DESCRIPCIÓN TÉCNICA

IDGT.TI.DOC.990

CONTENIDO

| | | |
|-------|---|----|
| 1 | INTRODUCCIÓN (OBJETIVO)..... | 3 |
| 2 | DESCRIPCIÓN DEL SOFTWARE..... | 4 |
| 2.1 | Componentes del Sistema..... | 4 |
| 2.2 | Arquitectura | 4 |
| 2.3 | Esquema de despliegue de la arquitectura | 4 |
| 2.3.1 | Sistema externo en modo Master | 5 |
| 2.3.2 | Sistema externo en modo Slave | 6 |
| 2.4 | Tecnologías..... | 7 |
| 2.5 | Lista de los servicios principales de Id-Gate..... | 7 |
| 3 | REQUISITOS DEL SOFTWARE Y EQUIPO..... | 9 |
| 3.1 | Servidor Id-Gate | 9 |
| 3.2 | Recomendaciones sobre el equipo | 10 |
| 3.2.1 | Recomendaciones sobre la instalación del terminal | 10 |
| 3.2.2 | Recomendaciones sobre la instalación de las cámaras | 10 |
| 4 | IDIOMAS DISPONIBLES | 12 |
| 5 | LISTA DE DOCUMENTACIÓN..... | 12 |
| 6 | DESARROLLADOR DE SOFTWARE | 12 |

1 INTRODUCCIÓN (OBJETIVO)

La solución Id-Gate es un producto de software diseñado para proporcionar una identificación precisa en los sistemas de control y gestión de acceso con el uso de la biometría.

Debido a la tecnología avanzada en su núcleo, Id-Gate amplifica significativamente las oportunidades de ACS, aumenta la confiabilidad de la identificación y hace que el acceso al territorio sea más rápido y fácil.

El sistema Id-Gate está diseñado para controlar el acceso a territorios e instalaciones mediante identificación biométrica. El sistema se puede integrar con sistemas de control de acceso, terminales y dispositivos biométricos en los puntos de control, así como con controladores, torniquetes y otros equipos de control de acceso

La Solución garantiza:

- Control de acceso al territorio debido a la identificación biométrica.
- Listas especializadas para las diferentes categorías de personas (VIP, listas de detención, etc.).
- Notificaciones instantáneas al servicio de seguridad cuando una persona no autorizada que no figure en la lista de acceso o, por ejemplo, esté en la "lista negra", intente entrar en el territorio.
- Análisis del número de visitantes y del tiempo que pasan en el territorio.
- Diferenciación de los derechos de acceso tanto de los empleados como de los visitantes a las distintas zonas del territorio.
- Integración con ACS, que reduce el riesgo de falsificación de la tarjeta de empleado, pérdida, transferencia a terceros, acceso de varias personas con una sola tarjeta.
- Sincronización de información personal: nombre completo, tarjetas de acceso, fotos, etc. La integración está disponible para los siguientes sistemas: Bosch Building Integration System, Honeywell Pro-Watch, Lenel OnGuard, Schneider Electric Security Expert, Dormakaba, Moxa, Robos.

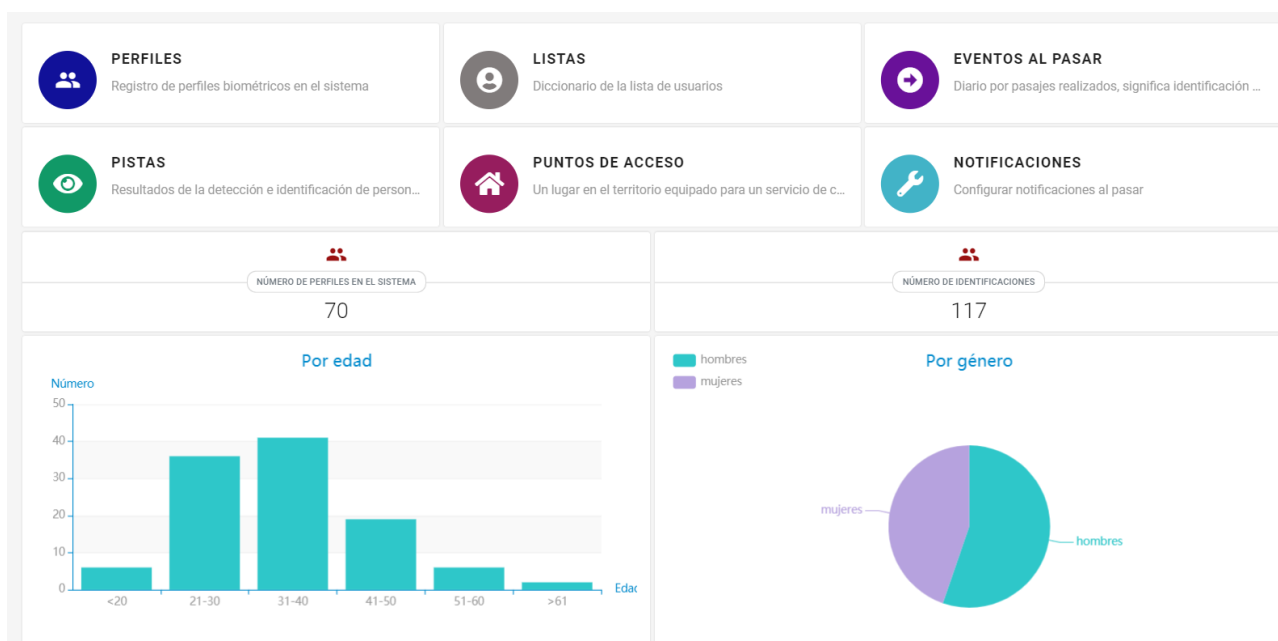


Imagen 1. Escritorio del Sistema

2 DESCRIPCIÓN DEL SOFTWARE

2.1 COMPONENTES DEL SISTEMA

Para el correcto funcionamiento del Sistema, se requiere el siguiente equipo mínimo:

- Servidor para el Núcleo de la Solución;;
- Servidor de preprocesamiento del vídeo (siempre que sea necesario);
- PC del Cliente (siempre que sea necesario);
- Cámaras de red o USB, en función de la finalidad y arquitectura de la Solución;
- Terminales de control de acceso;
- Conmutadores de red para la transmisión de datos entre los componentes del sistema.

La descripción detallada de las características recomendadas del equipo se indica a continuación.

2.2 ARQUITECTURA

El Sistema incluye los siguientes elementos:

- **Id-Gate Core** — la parte del servidor del sistema, que consta de servicios separados, incluyendo la interfaz de configuración del Sistema, algoritmos de reconocimiento, base de datos e informes.
- **Id-Gate Tracker** — servidor de preprocesamiento de vídeo.
- **Adaptador ACS** — servicio que proporciona el intercambio de datos entre los sistemas y el envío de notificaciones.
- **Aplicación Id-Gate** — componente del sistema utilizado para la integración con los terminales en los puestos de control y el control de acceso en modo offline.

El Sistema se puede integrar con:

- ACS
- Relé de torniquete u otros dispositivos de control de acceso
- Terminales
- Wiegand

A continuación se presentan esquemas de arquitectura del sistema para diferentes casos de uso.

2.3 ESQUEMA DE DESPLIEGUE DE LA ARQUITECTURA

Antes de desplegar la Solución y configurar la integración con un ACS, es necesario determinar las principales fuentes de datos maestros, en función de los algoritmos previstos de funcionamiento del Sistema en general. A saber: determinar dónde se introducirán los datos primarios, en qué orden y con qué sistemas deben sincronizarse. En general, Id-Gate permite configurar la integración definiendo los sistemas externos conectados en modo Master, Slave y combinado.

2.3.1 SISTEMA EXTERNO EN MODO MASTER

Para los casos en los que el ACS está integrado es la Fuente En los casos en los que el ACS que se está integrando es la fuente de datos maestros sobre perfiles, tarjetas de acceso e imágenes de perfil, se activa el modo Master en los ajustes de Id-Gate para el adaptador ACS del ACS correspondiente. Para la dicha integración, existe un intercambio bilateral de datos entre los sistemas. A continuación se muestra el esquema de una solución de este tipo (**Imagen 2**).

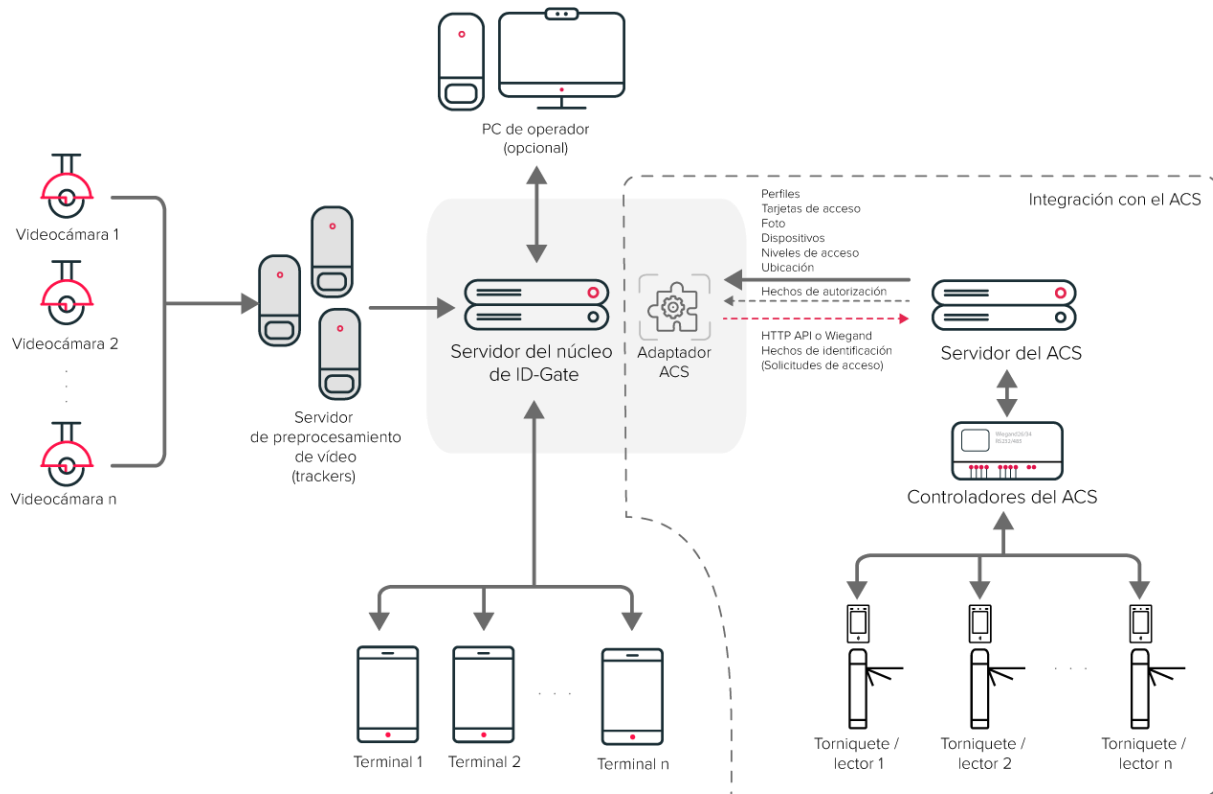


Imagen 2. Esquema de integración de Id-Gate con sistemas externos en modo Master

Bajo el ACS, se renueva constantemente una base de datos de empleados y visitantes con fotos y tarjetas de identificación, información sobre la ubicación de los actuadores, niveles de acceso, así como datos sobre los lectores y controladores. La información del ACS, como resultado de la sincronización periódica, es recibida por Id-Gate, actualizando la información sobre los dispositivos, las ubicaciones de los actuadores, los perfiles y los niveles de acceso.

Bajo Id-Gate, en tiempo real se procesan los flujos procedentes de las cámaras de seguridad conectadas al Sistema, así como los de los terminales. Tras los resultados del subsistema biométrico se ejecuta la identificación de todas las personas detectadas en la base de datos de perfiles que está sincronizada con el ACS. Los hechos de identificación que surgen se comprueban de acuerdo con las reglas configuradas, niveles de acceso por dispositivos, y como resultado del procesamiento se generan los hechos de identificación y se envían al ACS. Dependiendo de la configuración, pueden ser comandos a través de la API HTTP o comandos por Wiegand para abrir los dispositivos de acceso (torniquetes, puertas, barreras) que están conectados al ACS.

2.3.2 SISTEMA EXTERNO EN MODO SLAVE

En los casos en que Id-Gate es la fuente de datos maestros sobre perfiles, tarjetas de acceso e imágenes de perfil, el sistema externo integrado se habilita en modo Slave. Para tal integración, se realiza un intercambio bilateral de datos entre los sistemas. El esquema de una solución de este tipo se muestra a continuación (**Imagen 3**).

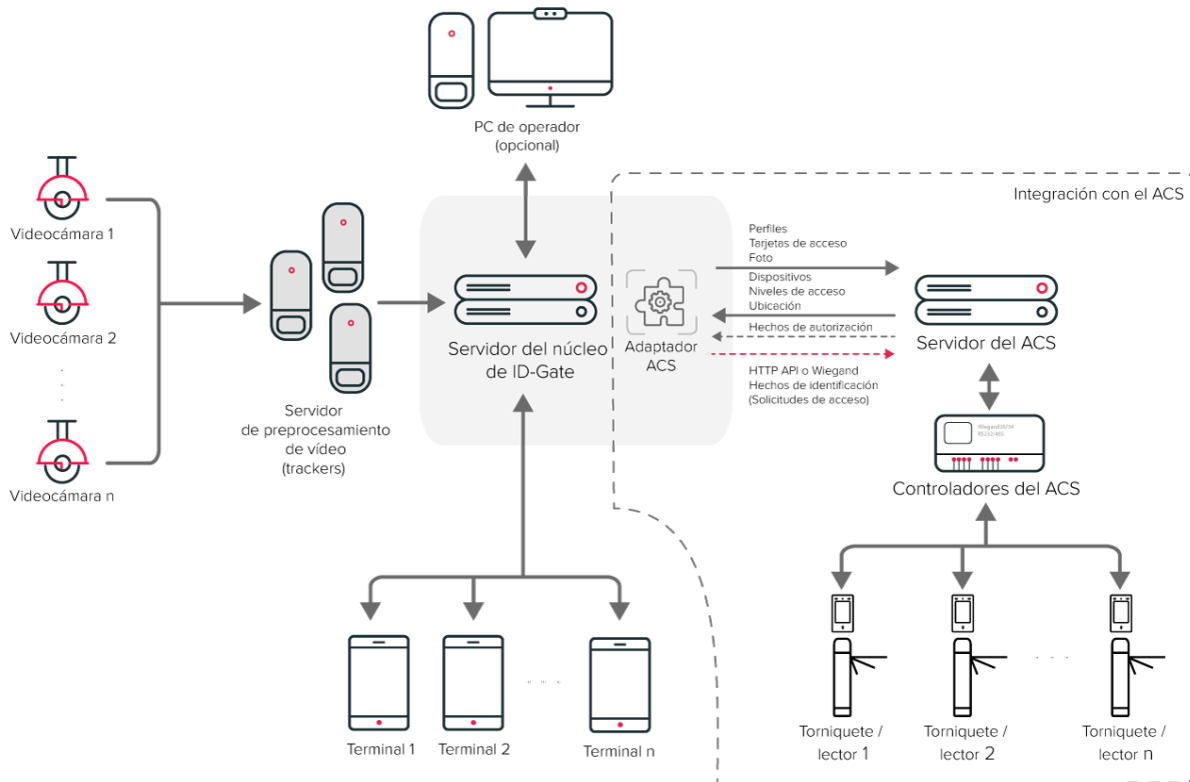


Imagen 3. Esquema de integración de Id-Gate con los sistemas externos en modo Slave

Bajo el Id-Gate, se renueva constantemente una base de perfiles con fotos y tarjetas de acceso. En tiempo real, se procesan los flujos de las cámaras de seguridad conectadas al Sistema, así como de los terminales. Tras los resultados del subsistema de biometría, se realiza la identificación de todas las personas detectadas.

Bajo el ACS, se carga información sobre los dispositivos (controladores, lectores, actuadores), la ubicación de los actuadores y los niveles de acceso. Como resultado de la sincronización periódica, la información sobre los derechos de acceso y los dispositivos se entrega a Id-Gate y debe aplicarse para formar reglas de manejo de hechos de identidad.

Los eventos de identificación que surgen en el lado de Id-Gate o los eventos de autorización recibidos del sistema externo se comprueban de acuerdo con el conjunto de reglas configuradas, los niveles de acceso por dispositivos, y como resultado del procesamiento se forman comandos para conceder o denegar el acceso que se envían al sistema externo. Dependiendo de la configuración, pueden ser comandos a través de la API HTTP o comandos por Wiegand para abrir los dispositivos de acceso (torniquetes, puertas, barreras) que están conectados al sistema externo.



Antes de configurar el sistema externo en modo Slave, debe realizarse siempre una copia de seguridad completa del ACS que se va a conectar. La solución Id-Gate que funciona en modo Master sustituirá automáticamente todos los datos del sistema conectado durante la primera sincronización.

2.4 TECNOLOGÍAS

El Sistema se desarrolla utilizando los siguientes lenguajes de programación:

- Golang
- C#
- Angular JS
- Rabbit MQ
- Nginx
- PostgreSQL
- Redis

2.5 LISTA DE LOS SERVICIOS PRINCIPALES DE ID-GATE

Id-Gate Core incluye los siguientes servicios:

Tabla 1. Servicios principales de Id-Gate

| Servicio | Descripción | Puerto |
|---------------------------------|--|----------------|
| Nginx | Un servidor web y un servidor proxy de correo | 80, 443, 23231 |
| Postgre SQL | El sistema de gestión de base de datos (SGBD) | 5432 |
| Rabbit MQ | Servicio para trabajar con colas de datos | 5672, 15672 |
| Redis | Sistema de gestión de bases de datos de clase NoSQL de código abierto | 6379 |
| mkvz-tracker-go | Servicio de preprocesamiento de flujos de vídeo (tracker) | 8001 |
| mkvz-tracker | Servicio de preprocesamiento de flujos de vídeo (tracker) | 8001 |
| mkvz-launcher | Servicio de Administración de Aplicaciones de Cliente | 8876 |
| mkv-server-report | Servicio de informes | 11084 |
| mu-server-api | Servicio de notificaciones | 11090 |
| support-server-api | Servicio de monitoreo que permite trabajar con métricas y escritorios | 11091 |
| mkv-server-url-shortener | Servicio de acortamiento de URL | 11092 |
| mas-server-api | Back-end para el modo de administración del sistema | 11101 |
| mas-server-settings | Servicio de configuraciones | 11102 |
| mpdn-secret-vault-api | Servicio de almacenamiento de datos personales | 11204 |
| mdc-server-api | Servicio para trabajar con clasificadores dinámicos | 11205 |
| mfs-server-api | Servicio para trabajar con archivos de foto | 11300 |
| mfs-server-thumbnail | Servicio para trabajar con miniaturas de fotos de almacenamiento de archivos | 11301 |
| fs-server-api | Servicio de almacenamiento de archivos | 11302 |
| mi-sender-email | Servicio de entrega por correo electrónico | 11400 |
| mi-sender-http | Servicio de envío de SMS mediante módem gsm USB | 11401 |
| mi-sender-smsmodem | Servicio de envío de SMS mediante módem gsm USB | 11402 |
| mi-server-api | Implementador de funciones API para trabajar con servicios | 11403 |
| mi-sender-telegram | Servicio de mensajería Telegram | 11404 |

| | | |
|--|---|-------|
| mi-controller-ac | Integrador empresarial e implementador de enrutamiento de solicitudes | 11406 |
| mi-adapter-ac-biostar2 | Adaptador de servicio de integración con ACS Biostar 2 | 11413 |
| mi-adapter-ac-moxa | Servicio de Adaptador de Integración Moxa 1214 | 11414 |
| mi-adapter-ac-suprema-fs2 | Adaptador del servicio | 11415 |
| mi-adapter-ac-honeywell-pro-watch | Adaptador de servicio de integración con ACS Honeywell Pro Watch | 11416 |
| mi-adapter-ac-bosch | Adaptador de servicio de integración con ACS Bosch BIS | 11417 |
| mi-adapter-ac-se | Adaptador de servicio de integración con ACS Security Expert | 11418 |
| mi-adapter-ac-exos | Adaptador de servicio de integración con ACS Dormakaba EXOS | 11421 |
| mi-adapter-ac-onguard | Servicio de adaptador de integración Lenel OnGuard ACS | 11422 |
| mi-adapter-ac-bolid | Servicio del adaptador | 11436 |
| mi-adapter-ac-go | Adaptador Test Go | 11444 |
| mkv-server-admin | Servicio de administración de usuarios del sistema | 11500 |
| mkv-server-api | Servicio de interacción de clientes | 11501 |
| mkv-server-auth | Servicio de Administración | 11502 |
| mkv-server-ws | Back-end para aplicación de cliente WebSocket | 11503 |
| backup-client-server-api | Servicio de copia de seguridad de datos del sistema | 11506 |
| logging-server-api | Servicio de registro | 11509 |
| event-configuration-api | Servicio de procesamiento de eventos del sistema | 11510 |
| event-storage-server-api | Servidor de procesamiento de eventos del sistema | 11511 |
| mkv-client-profiles-import | Servicio de importación de perfiles | 11514 |
| mas-meta-server-api | Servicio de información meta | 11515 |
| monitoring-server-api | Servicio de monitorización | 11517 |
| statistics-server-api | Servicio de mantenimiento de estadísticas sobre el funcionamiento del sistema | 11518 |
| audit-server-api | Servicio de auditoría y registro | 11521 |
| mkv-server-auth-ldap | Servicio de autorización en el sistema a través de LDAP/AD | 11522 |
| discovery-server-api | Servicio de búsqueda de aplicaciones móviles DSN-SD | 11551 |
| adb-server-api | Servicio de Administración de Aplicaciones Móviles a través del protocolo UDP | 11552 |
| mas-server-report | Servicio de informes para MAS | 11553 |
| medical-server-api | Servicio de control médico | 11554 |
| mmpd | Gestor de servicios para procesos de detección | 11600 |
| mobile-service-api | API para trabajar con aplicaciones móviles | 11601 |
| gate-server-api | Servicio de procesos de concesión de acceso | 11602 |
| compromise-server-api | Servicio del control de compromiso | 11605 |
| modi-image-worker | Servicio de procesamiento de fotos | 11700 |
| modi-server-api | Servicio de procesamiento de imágenes discretas | 11701 |

| | | |
|---------------------------------|---|---|
| modi-ubda-tevian-[01-04] | Servicio de procesaminto de fotos | 11710 y [01], 11711 y [02], 11712 y [03], 11713 y [04] |
| modi-ubda-tevian-alg1 | Servicio de procesaminto de fotos | 11714 |
| mrp-server-api | Servicio de preprocesamiento de datos | 11800 |
| mrp-matching-tevian-go | Servicio de correspondencia para Tevian | 11806 |
| mrp-server-broker | Servicio de gestión | 11821 |
| mrp-server-image-broker | Servicio de distribución de imágenes para trackers | 11822 |
| ms-server-filecache | Servicio de almacenamiento en caché | 11900 |
| mkv-scheduler-api | Servicio que implementa trabajo con tareas planificadas | 11910 |
| video-restreamer-server | Servicio de Retransmisión de Vídeo | 40000, 40001 |

Uno de los requisitos del servidor para instalar el software Id-Gate Core es que el servidor no tenga el software antes especificado en la tabla y que haya puertos libres especificados en la tabla.

3 REQUISITOS DEL SOFTWARE Y EQUIPO

3.1 SERVIDOR ID-GATE

El procesamiento de la información de la biometría facial requiere muchos recursos computadores. Las características del servidor dependen directamente de la cantidad de información procesada por el Sistema recibida de las cámaras. En la Tabla 2 se presenta un cálculo aproximado de los valores más frecuentes.

Tabla 2. Requisitos del servidor

| Número de cámaras | CPU (Core) | RAM (GB) | HDD (GB) | SSD (GB) |
|-------------------|------------|----------|----------|----------|
| 1 | 5 | 16 | 600 | 240 |
| 2 | 6 | 16 | 700 | 240 |
| 3 | 8 | 16 | 700 | 240 |
| 5 | 10 | 32 | 800 | 240 |
| 7 | 14 | 32 | 900 | 240 |
| 10 | 18 | 64 | 1000 | 240 |

Sistema operativo: Windows 10 Pro (2004 y más tarde, de acuerdo con la fecha límite para el fin de soporte para los sistemas operativos), Windows Server 2016/2019 y más tarde. Si tiene instalada la edición del SO "Windows 10 Pro N", deberá instalar adicionalmente el componente "Media Feature Pack". La cuenta (nombre de usuario/contraseña) (incluso para un usuario remoto) debe permanecer sin cambios durante toda la instalación. La cuenta (nombre de usuario/contraseña) debe permitir la actualización de privilegios a Administrador si es necesario.

Los siguientes componentes no se deben preinstalar en el servidor:

- Postgre SQL
- Rabbit MQ
- Redis
- Web server utilizado 80 y 443 puertos

3.2 RECOMENDACIONES SOBRE EL EQUIPO

3.2.1 RECOMENDACIONES SOBRE LA INSTALACIÓN DEL TERMINAL

Si el terminal se instala en el interior, el dispositivo debe colocarse a una distancia de al menos 2 metros de la fuente de luz (para evitar el deslumbramiento y los brillos) y al menos 0,3-0,5 metros de la ventana o la puerta. (Imagen 3). Al instalar el terminal es recomendable evitar los siguientes factores:

- Deslumbramiento masivo que procede de atrás;
- Exposición del terminal a la luz solar directa;
- Cercanía a fuentes de luz brillantes.

La superficie de montaje debe ser capaz de soportar el doble del peso del equipo.

La altura de instalación del terminal recomendable es 1,45-1,55 m desde el nivel del suelo hasta el módulo de la cámara incorporado en el terminal. La altura de instalación del terminal es la recomendada y puede modificarse para adaptarla a sus necesidades.

Durante la instalación, es necesario garantizar la seguridad del equipo y de las herramientas de instalación utilizadas.

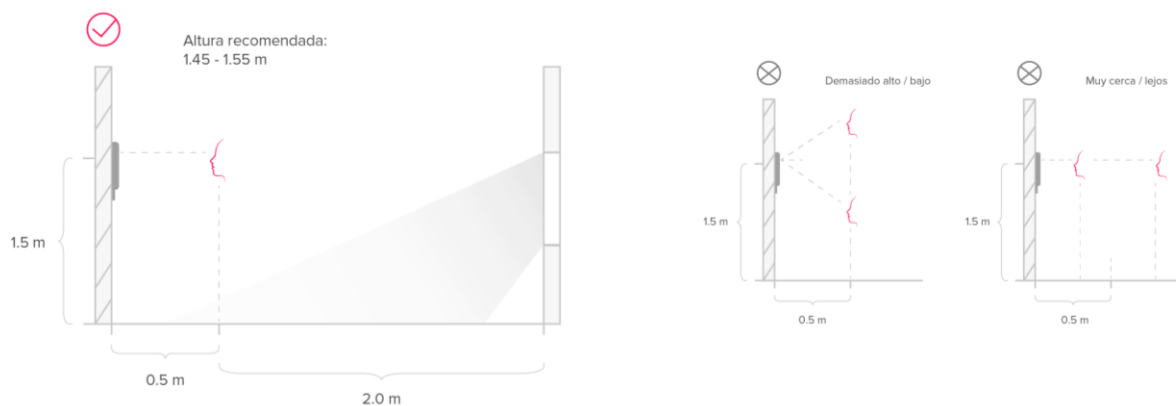


Imagen 4. Recomendaciones sobre la instalación de los terminales

3.2.2 RECOMENDACIONES SOBRE LA INSTALACIÓN DE LAS CÁMARAS

- La cámara debe fijarse rígidamente con un soporte especial para minimizar el efecto de desenfoque causado por el movimiento de la cámara. La cámara también puede montarse en un trípode a una altura de entre 1,5 m y 2 m.
- Colocación recomendada de la cámara. El objetivo de la cámara debe apuntar hacia la dirección de las personas para que los objetos se muevan en la dirección de la cámara a lo largo de la línea de visión.
- La trayectoria del movimiento de una persona no debe ser bloqueada por las pantallas, los mostradores de información, señalización o pancartas.
- Para mejor reconocimiento e identificación es preferido usar las cámaras de vídeo con lentes varifocales.
- La distancia focal del objetivo preferida es entre 9 y 40 mm.
- El ángulo de inclinación de la cámara al final del área de detección facial debe estar dentro de 15 grados.
- La altura óptima de montaje de la cámara es de 2,2 metros por encima del suelo y, preferiblemente, de 8,0 a 8,5 metros por debajo del inicio de la zona de detección facial.
- Es necesario que el interior del local sea iluminado de manera igual y constante. Para garantizar el reconocimiento facial óptimo, la iluminación difusa debe ser tal que los rostros de las personas estén

iluminados igualmente, sin sombras ni deslumbramientos. La intensidad luminosa recomendada es de unos 300 lux (con el mínimo de 150 lux y el máximo de 600 lux).

- En la posición inicial de detección de rostros, la cámara debe configurarse y ajustarse de modo que el tamaño de la cara de un adulto sea de 160 x 160 píxeles (el campo de visión es de más de 2 metros de ancho, es decir, un poco más ancho que la distancia de los brazos extendidos a los lados).

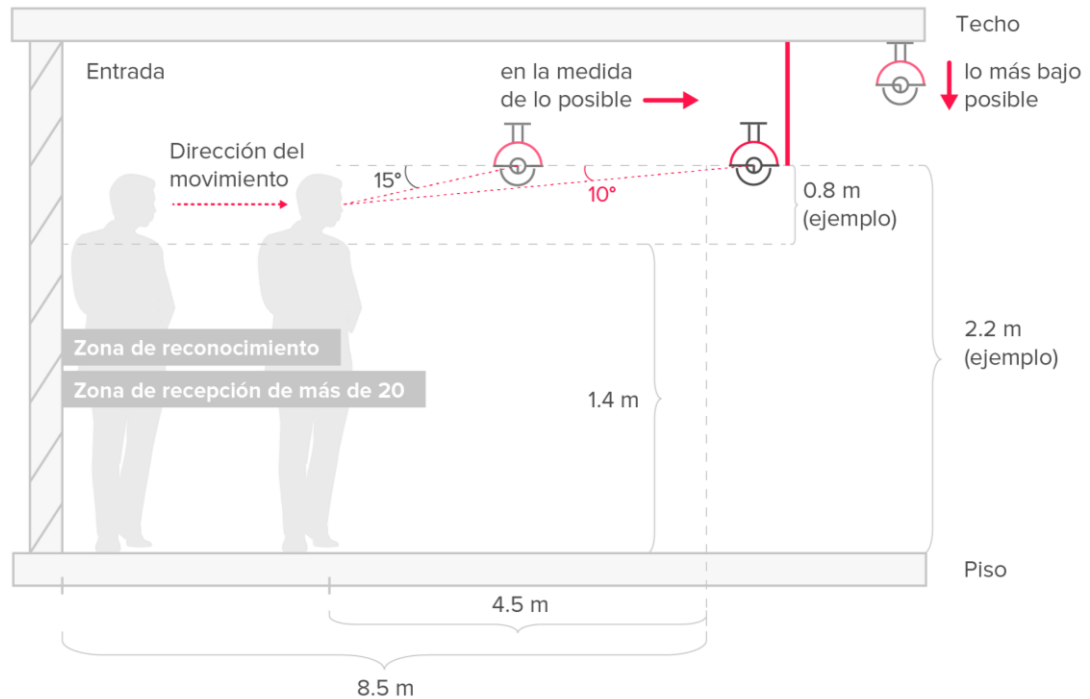


Imagen 5. Recomendaciones sobre la instalación de las cámaras

4 IDIOMAS DISPONIBLES

El software Id-Gate es una solución multilingüe que le permite elegir entre varias opciones de idiomas.

Idiomas disponibles:

- Inglés (por defecto)
- Español

La lista de idiomas disponibles puede ampliarse previa solicitud.

5 LISTA DE DOCUMENTACIÓN

- Guía del Administrador de Id-Gate
- Guía del Operador de Id-Gate
- Guía del usuario de la aplicación Android para terminales

6 DESARROLLADOR DE SOFTWARE

RecFaces FZ-LLC

Dirección: Dubai Internet City Edificio 3, Dubai, EÁU

Teléfono: +971 4 8368339

Correo electrónico:

- Cuestiones: in@recfaces.com
- Programa de licencias y socios: sales@recfaces.com
- Cuestiones técnicas y soporte de productos: id-gate@recfaces.com