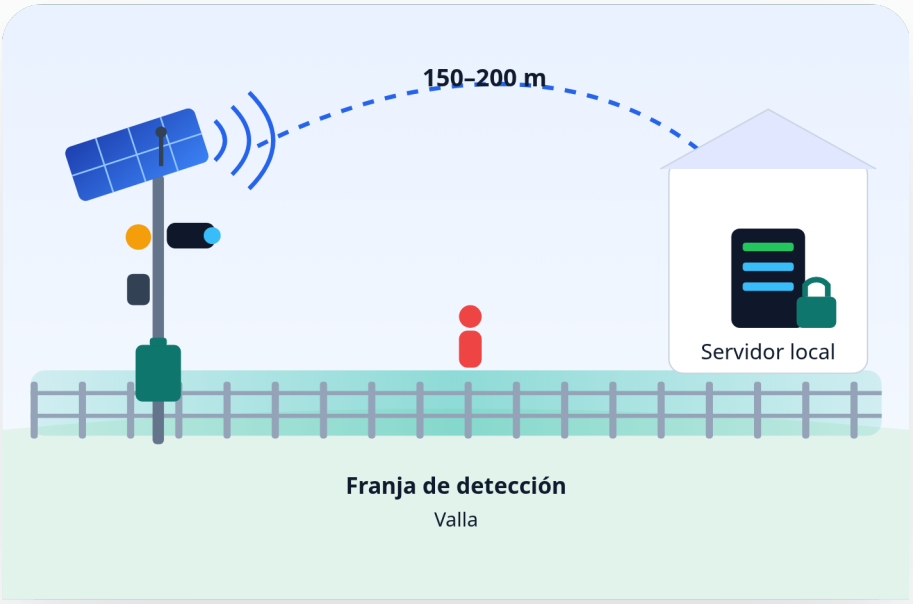
SEGURIDAD DE LA ZONA COMÚN DE LA COMUNIDAD

CLARYEL Perimetro

Proyecto de un sistema inteligente y autónomo de protección de la zona común

Un único punto autónomo de videovigilancia inteligente a lo largo de la valla. Todos los datos se quedan solo con nosotros, dentro de la comunidad, cifrados: sin nubes, sin servicios de terceros, todo solo en local.

- Solo en local
- Cifrado
- Sin nube
- Bloqueo inmediato ante cualquier alarma



PRINCIPIO FUNDAMENTAL

Todo se queda con nosotros, dentro de la comunidad

Todas las imágenes, los fragmentos de eventos y los registros se guardan solo en el servidor local dentro del edificio, en la comunidad.

Toda la información se guarda y se transmite cifrada.

Ante cualquier alarma, toda la información puede bloquearse al instante: se cierra el acceso al archivo y los fragmentos del evento quedan protegidos contra modificación y borrado.

Sin nubes y sin servicios de terceros: el procesamiento con inteligencia artificial y el almacenamiento se realizan solo en local.

- Servidor local en el edificio
- Cifrado
- Bloqueo inmediato
- Sin nube
- Sin servicios de terceros



ALTERNATIVA A LA CÁMARA

Detección mediante señales Wi-Fi: sin imágenes, sin identificación

- Sin cámara
- Sin imágenes
- Sin identificación
- Solo en local

Como alternativa a la cámara, pueden instalarse dos dispositivos Wi-Fi a lo largo de la valla, uno en cada extremo del tramo vigilado.

A partir de los datos en bruto de la señal Wi-Fi entre los dos dispositivos (sus variaciones, conocidas como CSI — Channel State Information), el sistema obtiene

los contornos de las personas que se mueven en la franja, sin ninguna imagen y sin identificar quiénes son.

La técnica ya se estudia en el interior de las viviendas: por ejemplo, la investigación «DensePose From WiFi» de la Universidad Carnegie Mellon reconstruye la silueta de las personas en una habitación usando solo señales Wi-Fi. Proponemos aplicarla en el exterior, a lo largo de la valla.

El sistema detecta solo la presencia, la dirección del movimiento y una silueta anónima. El procesamiento se realiza en el servidor local, cifrado, como en el resto del proyecto, y activa los mismos avisos: luz, mensaje de voz y notificaciones a los residentes.

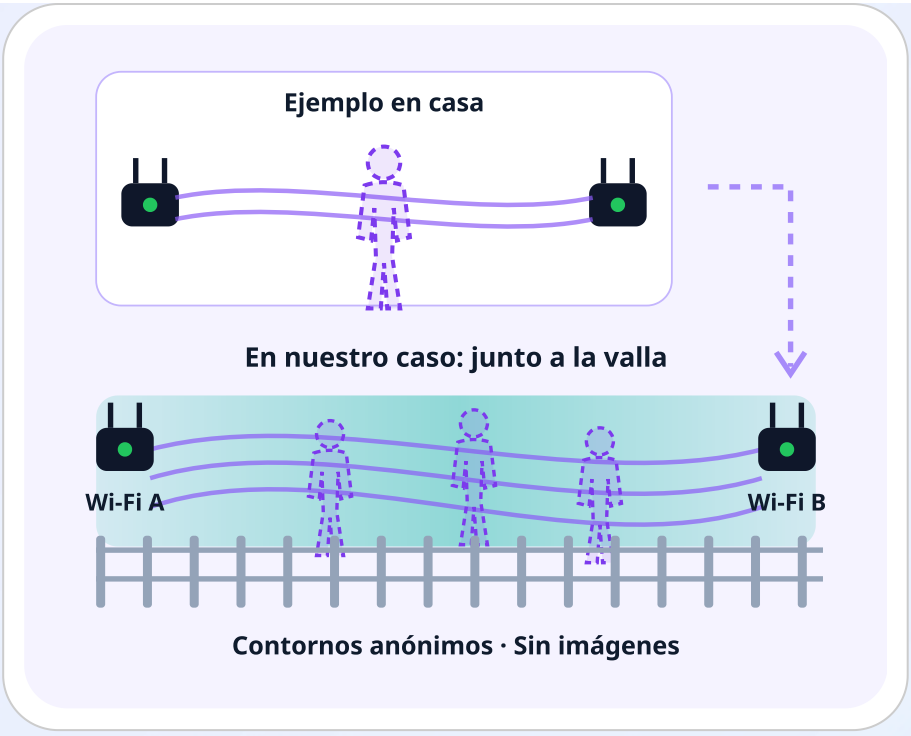
Aspectos jurídicos — a verificar con el DPO o con un asesor

La detección Wi-Fi no capta imágenes ni vídeo: por lo tanto, no es un sistema de videovigilancia, y las normas específicas sobre videovigilancia (por ejemplo, el cartel informativo indicado por el Garante para las cámaras) no se aplican como tales.

No obstante, el RGPD sigue siendo aplicable si los datos pueden referirse a una persona identificada o identificable (art. 4, apartado 1, del RGPD). Por eso el sistema está diseñado para tratar solo la presencia y contornos anónimos, sin identificación, solo en local y de forma cifrada.

Esta valoración debe confirmarse con el DPO o con un asesor antes de la instalación y no constituye una garantía jurídica.

Ejemplo en una vivienda: «DensePose From WiFi», Universidad Carnegie Mellon (arXiv) ↗



01

Finalidad del proyecto

Se propone instalar un único punto autónomo de videovigilancia inteligente a lo largo de la valla de la zona común de la comunidad.

El sistema está pensado para detectar una posible intrusión no autorizada, advertir a los infractores e informar rápidamente a los vecinos.

Principios fundamentales del proyecto:

01

Mínima intromisión en la vida privada.

02

Vigilancia solo de una franja estrecha a lo largo de la valla.

03

Procesamiento de imágenes con inteligencia artificial totalmente en local.

04

Sin servicios en la nube obligatorios.

05

Cifrado de la información transmitida y almacenada.

06

Avisos automáticos y notificaciones a los vecinos.

07

Posibilidad de dirigirse rápidamente a las fuerzas de seguridad.

02

Limitación de la videovigilancia y protección de la privacidad

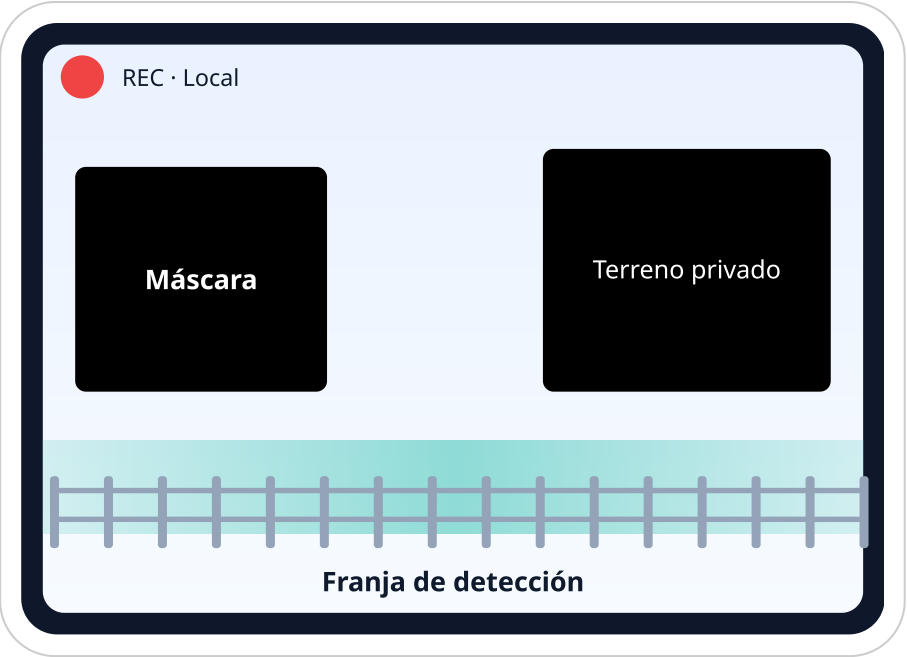
La cámara apuntará exclusivamente a un tramo predefinido de la zona común, directamente a lo largo de la valla.

Cualquier parte de la imagen en la que puedan aparecer parcelas privadas vecinas, ventanas, balcones y otros espacios ajenos a la zona controlada quedará totalmente cubierta con máscaras negras opacas.

El enmascaramiento se realiza directamente en la cámara, antes de la transmisión y grabación del flujo de vídeo.

Además, por software se define una franja de detección estrecha. La inteligencia artificial no analizará objetos fuera de esta área.

El sistema no contempla reconocimiento facial, identificación de personas concretas, control de vehículos ni observación de la vida cotidiana de los vecinos.



03

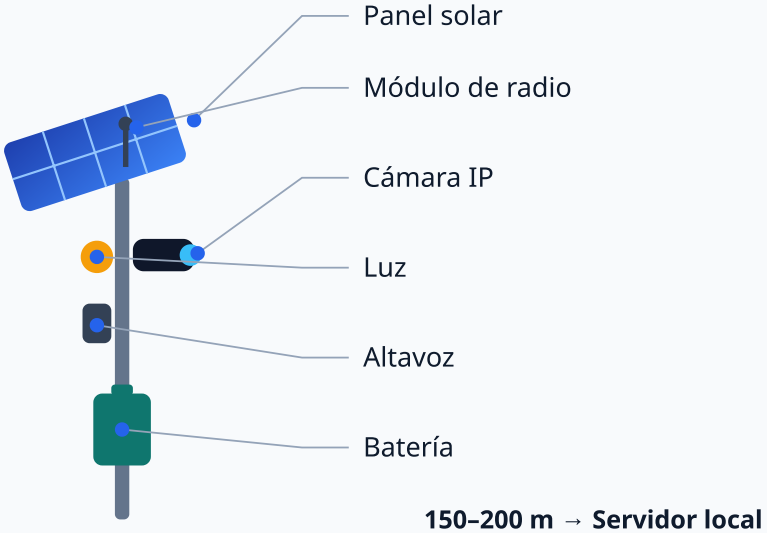
Equipo autónomo

El nodo remoto contará con una cámara IP, un panel solar, una batería, un módulo de comunicación inalámbrica, un indicador luminoso y un pequeño altavoz.

La distancia prevista hasta el servidor local es de 150–200 metros.

La imagen se transmitirá por un enlace inalámbrico seguro a un servidor situado dentro del edificio.

El funcionamiento del sistema no dependerá de internet externo. Internet solo será necesario para enviar notificaciones fuera de la red local y para un posible contacto con las fuerzas de seguridad.



04

Inteligencia artificial local

En el servidor local funcionará un algoritmo especializado de visión artificial.

De forma preliminar se prevé analizar la imagen a dos fotogramas por segundo, con la posibilidad de aumentar la frecuencia si fuera necesario.

El sistema distinguirá a las personas del movimiento de árboles, arbustos, animales, lluvia y otros cambios naturales de la imagen.

Los avisos solo se activarán ante la detección confirmada de una persona en la zona establecida.

Además, se puede analizar la dirección del movimiento, el cruce de un límite virtual y el tiempo de permanencia en la franja vigilada.



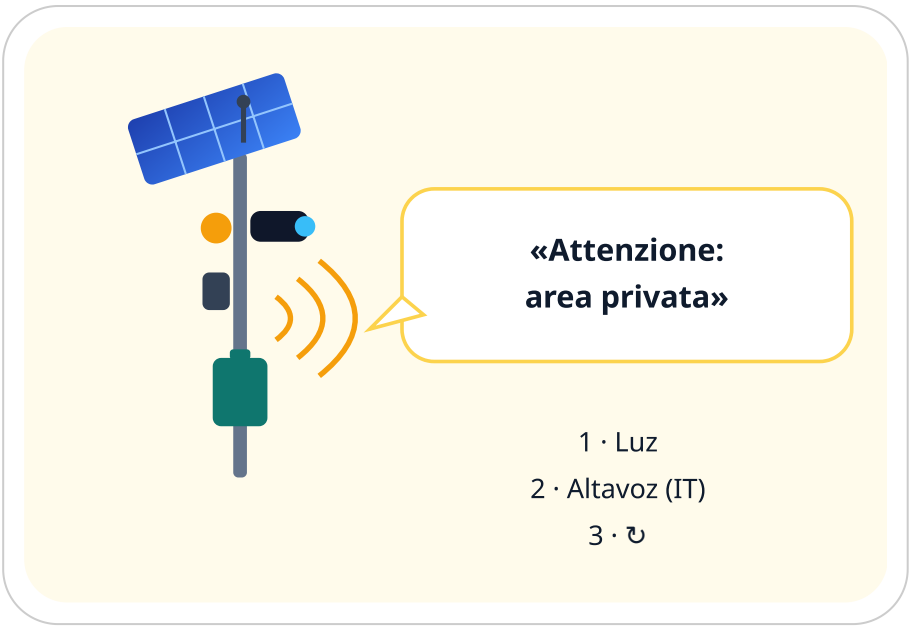
05

Aviso automático en el lugar

Cuando aparezca una persona en la zona protegida, el sistema podrá:

1. Encender un indicador luminoso de aviso.
2. Reproducir un mensaje de voz en italiano indicando que se encuentra en una propiedad privada.
3. Si es necesario, repetir el aviso dentro de los límites establecidos.

El volumen, el horario de funcionamiento y las condiciones de activación se ajustarán para reducir al mínimo las molestias a los vecinos.



06

Notificaciones a todos los vecinos

Todos los vecinos interesados podrán recibir notificaciones en su teléfono móvil sin que se envíen fotos ni imágenes de vídeo.

Por ejemplo:

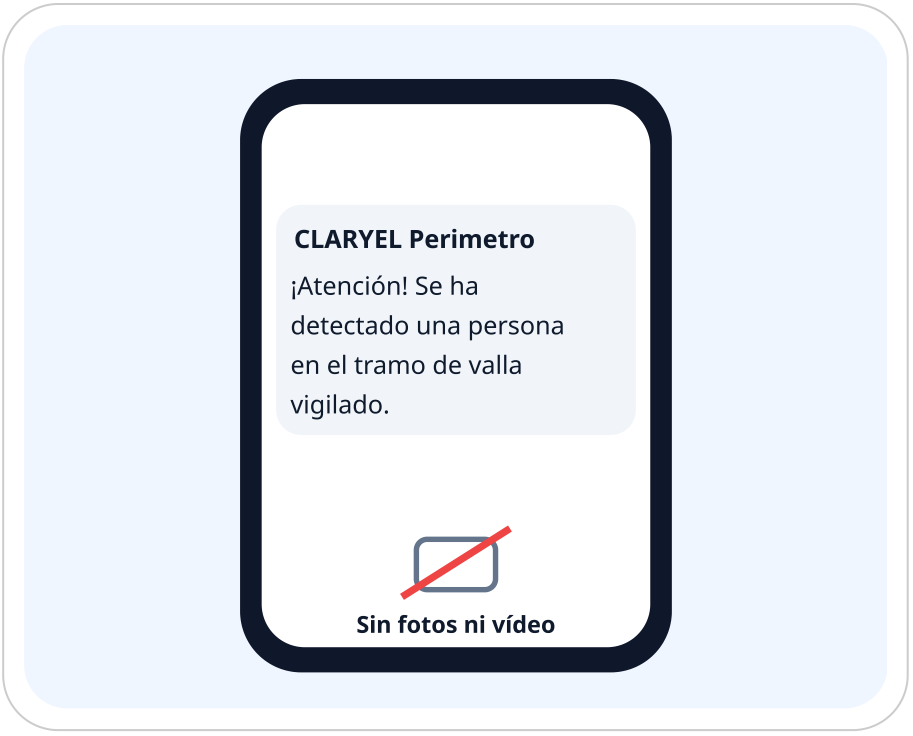
> **«¡Atención! Se ha detectado una persona en el tramo de valla vigilado. El sistema ha activado un aviso».**

Para recibir las notificaciones habituales, los vecinos no necesitarán acceso a la cámara ni al archivo.

La suscripción a las notificaciones será voluntaria. Cada participante podrá renunciar a recibir mensajes.

El administrador del sistema gestionará solo la lista de destinatarios y la configuración de las notificaciones.

El envío se organizará respetando los requisitos de protección de los datos de contacto de los participantes.



07

Reacción ante una intrusión confirmada

Se prevé un modo adicional de alerta elevada.

Puede activarse si el sistema detecta una secuencia de indicios de una posible intrusión, por ejemplo:

- Una persona ha cruzado el límite establecido de la valla.
- Sigue avanzando hacia el interior del recinto.
- Se encuentra en una zona por la que normalmente no deberían pasar personas.
- El evento está confirmado por el análisis de varios fotogramas.

En ese caso, el sistema podrá guardar automáticamente un fragmento de vídeo y enviar una notificación urgente a los vecinos.

Posibilidad de avisar a la policía

La arquitectura técnica prevé la posibilidad de preparar un mensaje automático para las fuerzas de seguridad.

Ante una intrusión confirmada, el sistema podrá preparar:

- Un mensaje de voz en italiano con la dirección, la naturaleza del evento y la hora de detección.
- Varias imágenes o un breve fragmento de vídeo.
- Información sobre el lugar del incidente.
- Datos de contacto del representante encargado de la comunidad.

Para casos de emergencia se prevé una llamada rápida a la policía a través de una persona encargada.

En el futuro podrá organizarse la transmisión de información e imágenes por correo electrónico, por un canal electrónico seguro u otro medio de comunicación acordado oficialmente.

Un aviso totalmente automático directamente a la policía solo es posible si existe un procedimiento de colaboración adecuado y acordado oficialmente. Hasta su aprobación, la llamada y la transmisión de imágenes se realizarán tras la confirmación de una persona encargada.

Esto es necesario para evitar avisos infundados debidos a errores técnicos o falsas alarmas.



Conservación de la información y gestión de accesos

Todo se queda solo en local, dentro de la comunidad, cifrado. Ante cualquier alarma, la información puede bloquearse al instante. Sin nubes y sin servicios de terceros.

El flujo de vídeo se procesará en el servidor local sin usar servicios externos de inteligencia artificial.

No se prevé la grabación continua de todo el flujo de vídeo. Si es necesario, se guardarán breves fragmentos relacionados con los eventos detectados.

De forma preliminar se propone el borrado automático de las grabaciones ordinarias a las 24 horas. Se admite una conservación más larga de un evento concreto cuando exista una necesidad justificada, por ejemplo para entregar material a las fuerzas de seguridad.

El acceso a las imágenes se concede solo a personas designadas expresamente.

Los vecinos reciben notificaciones escritas, pero no acceso a la cámara.

Todos los accesos al archivo quedan anotados en el registro del sistema.



Aprobaciones necesarias

Para la realización se propone el siguiente procedimiento:

Primera fase — debate con los vecinos.

Publicación de la descripción técnica del proyecto y recogida de observaciones.

Segunda fase — acuerdo con la administración.

Al administrador de la comunidad se le entregan la descripción del sistema, el plano de ubicación de la cámara, el esquema de limitación de la zona vigilada y las normas de tratamiento de datos.

Tercera fase — acuerdo de la junta.

La instalación del equipo en la zona común se somete a votación de conformidad con los artículos 1122-ter y 1136 del Código Civil italiano.

Cuarta fase — elaboración de las normas de uso.

La comunidad se designa como responsable del tratamiento de los datos. Si es necesario, se nombra un operador técnico del sistema con facultades limitadas.

Se aprueban las normas de acceso, los plazos de conservación, el procedimiento de notificación a los vecinos y el uso de las grabaciones.

Se instalan los carteles informativos obligatorios sobre videovigilancia.

Quinta fase — funcionamiento experimental.

Tras obtener las autorizaciones necesarias, se instala un único punto experimental. Se comprueban la fiabilidad de la detección, las falsas alarmas, la calidad del enlace, la alimentación y el funcionamiento de las notificaciones.

El envío de mensajes directamente a las fuerzas de seguridad se estudia por separado con los servicios competentes.

10

Conclusión

El sistema propuesto es un conjunto de seguridad inteligente y autónomo, destinado exclusivamente al control de un tramo limitado de la zona común.

Su tarea no es observar a los vecinos, sino detectar a tiempo una posible intrusión a través de la valla, advertir al infractor e informar a los residentes.

El procesamiento local con inteligencia artificial, la limitación del campo de visión, el enmascaramiento físico de las zonas privadas y la ausencia de libre acceso a las grabaciones deberían garantizar un alto nivel de protección de la privacidad.

En el futuro el sistema podrá completarse con medios de colaboración rápida con las fuerzas de seguridad.

El proyecto está pensado para realizarse de forma gradual, empezando por un único punto experimental y solo después de las aprobaciones necesarias.



Local · Máscara · Cifrado

+

Propuestas de mejora

A continuación, las propuestas de CLARYEL para debatir con los vecinos y la administración. No forman parte del proyecto aprobado ni son un dictamen jurídico: cada propuesta debe comprobarse con el administrador y, si es necesario, con un especialista en protección de datos.

PROPUESTA PARA DEBATIR · 1

Evaluación de impacto en la protección de datos

Antes de la instalación, realizar y documentar una evaluación de impacto (EIPD, art. 35 RGPD) o justificar por escrito por qué no es necesaria en este caso.

PROPUESTA PARA DEBATIR · 2

Información a vecinos y transeúntes

Colocar el cartel informativo según el modelo del Garante Privacy para videovigilancia y preparar la información completa del art. 13 RGPD, teniendo en cuenta las indicaciones del Garante y del CEPD sobre videovigilancia.

PROPUESTA PARA DEBATIR · 3

Política de conservación por escrito

Fijar en las normas: 24 horas por defecto, la lista de excepciones admitidas, quién decide la prórroga y cómo se borra una grabación prorrogada.

PROPUESTA PARA DEBATIR · 4

Horas de silencio y límites del altavoz

De noche, solo luz o volumen reducido, un número máximo de repeticiones por evento y una pausa entre avisos.

PROPUESTA PARA DEBATIR · 5

Control de manipulaciones y averías

Avisos separados al administrador si la cámara se tapa o se mueve, si cambia el encuadre, si el nodo no responde o si la batería se está agotando.

PROPUESTA PARA DEBATIR · 6

«Latido» del nodo

El nodo envía regularmente al servidor una señal de funcionamiento; si falta la señal, el administrador recibe un mensaje.

PROPUESTA PARA DEBATIR · 7

Protección del enlace y del almacenamiento

Cifrado del enlace de radio (por ejemplo WPA3 y túnel WireGuard), almacenamiento cifrado de fragmentos, registro de accesos, actualizaciones del firmware de la cámara y cambio de las contraseñas de fábrica.

PROPUESTA PARA DEBATIR · 8

Acceso de dos personas

Visionado y exportación de fragmentos solo con la participación de dos personas designadas, con anotación en el registro.

PROPUESTA PARA DEBATIR · 9

Comprobación de máscaras antes del arranque

Mostrar a los vecinos un fotograma con las máscaras aplicadas y adjuntarlo al acta de la junta antes de la puesta en marcha; repetir tras cualquier nuevo ajuste de la cámara.

PROPUESTA PARA DEBATIR · 10

Indicadores de la fase experimental

Registrar falsas alarmas y detecciones fallidas, acordar de antemano criterios de «seguimos / no seguimos» y presentar un informe a la junta.

PROPUESTA PARA DEBATIR · 11

Canales de notificación

Las notificaciones se generan en el servidor local y solo contienen un mensaje escrito, sin imágenes; la junta elige el medio de envío, dando preferencia a opciones sin servicios en la nube de terceros; es posible darse de baja en cualquier momento.

PROPUESTA PARA DEBATIR · 12

Minimización de datos

Sin reconocimiento facial, sin lectura de matrículas, sin grabación de audio; guardar solo lo necesario para el evento concreto.

PROPUESTA PARA DEBATIR · 13

Autonomía en invierno

Comprobar la reserva de energía del panel solar y de la batería en los días cortos y nublados y definir de antemano el comportamiento del nodo con batería baja.

PROPUESTA PARA DEBATIR · 14

Ubicación de los carteles

Los carteles se colocan antes de la entrada a la zona grabada y son bien visibles de día y de noche.

PROPUESTA PARA DEBATIR · 15

Revisión periódica

Presentar regularmente a la junta, por ejemplo una vez al año, un informe sobre el funcionamiento del sistema, la configuración de la zona y los plazos de conservación.

PROPUESTA PARA DEBATIR · 16

Modelo de aviso para la policía

Un formulario preparado de antemano: fecha y hora, tramo, descripción, fragmentos, contacto del representante encargado, quién confirmó el evento y cuándo.

?

Preguntas frecuentes

¿La cámara grabará ventanas, balcones y terrenos privados?

No. Esas partes de la imagen se cubren con máscaras negras opacas directamente en la cámara, antes de la transmisión y la grabación. La inteligencia artificial solo analiza una franja estrecha a lo largo de la valla.

¿Quién puede ver los vídeos?

Solo personas designadas expresamente. Los vecinos reciben notificaciones escritas sin fotos ni vídeo y no tienen acceso a la cámara ni al archivo. Cada acceso al archivo queda registrado.

¿Dónde se guardan los datos y durante cuánto tiempo?

Solo en el servidor local dentro de la comunidad, cifrados, sin nube ni servicios de terceros. No hay grabación continua: los breves fragmentos de eventos se borran, de forma preliminar, automáticamente a las 24 horas; una conservación más larga solo ante una necesidad justificada.

¿Puedo renunciar a las notificaciones?

Sí. La suscripción es voluntaria y puede dejar de recibir mensajes en cualquier momento.

¿Y las falsas alarmas?

El sistema distingue a las personas de árboles, arbustos, animales y lluvia, y los avisos solo se activan ante la detección confirmada de una persona. A la policía se la avisa solo tras la confirmación de una persona encargada. Las falsas alarmas se comprueban en la fase experimental.

¿El sistema reconocerá caras o matrículas?

No. El proyecto no contempla reconocimiento facial, identificación de personas concretas ni control de vehículos.

¿Cuánto costará?

El coste aún no está definido. Se debatirá por separado, después de acordar las soluciones técnicas con los vecinos y la administración.

§

Referencias normativas

Fuentes oficiales útiles para el debate. Los enlaces son informativos y no sustituyen el asesoramiento de un profesional.

Reglamento (UE) 2016/679 (RGPD) — versión oficial ↗ — https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679
En particular, art. 13 (información) y art. 35 (evaluación de impacto).

Código italiano de protección de datos personales — D.Lgs. 196/2003 ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196
Normattiva, versión vigente.

Código Civil italiano, art. 1122-ter — instalaciones de videovigilancia en elementos comunes ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1942-03-16;262~art1122ter
Normattiva.

Código Civil italiano, art. 1136 — constitución de la junta y validez de los acuerdos ↗ — https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1942-03-16;262~art1136
Normattiva.

Garante Privacy — Videovigilancia ↗ — https://www.garanteprivacy.it/temi/videosorveglianza
Página temática de la autoridad italiana de protección de datos.

Garante Privacy — FAQ sobre videovigilancia, guía y modelo de cartel ↗ — https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9496574
Indicaciones sobre la información simplificada (cartel) y los plazos de conservación.

CEPD — Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo ↗ — https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_it
Comité Europeo de Protección de Datos.

Ámbito local

La comunidad se encuentra en el municipio de Fino Mornasco (provincia de Como). Los organismos indicados abajo son posibles interlocutores para la coordinación: el proyecto no supone ningún acuerdo ya firmado con ellos.

En cualquier emergencia sigue vigente el número europeo de emergencias 112.

Municipio de Fino Mornasco ↗ — https://www.comune.finomornasco.co.it/
Administración municipal y Policía Local (Polizia Locale): coordinación sobre normas locales y carteles.

Arma dei Carabinieri ↗ — https://www.carabinieri.it/
El puesto territorialmente competente: posible procedimiento acordado para los avisos.

✉

Tu propuesta u observación

La primera fase del proyecto es el debate con los vecinos. Escríbenos qué mejorar y qué te genera dudas o preguntas.

O escríbenos directamente

CLARYEL Perimetro — Este es un proyecto para debatir con los vecinos y la administración de la comunidad. Su realización solo es posible tras las aprobaciones necesarias.

Los contenidos son meramente informativos y no constituyen asesoramiento jurídico.

CLARYEL SRLS · Fino Mornasco (CO) · P.IVA 04258140138 · Sitio de CLARYEL: claryel.com