

VIDEO · INTRUSION · ACCESS CONTROL · NETWORK

Security system network

We design the network that carries images, alarms and door events: segmentation, PoE, backup power, secure remote access and explicit rules between networks. Your team sees the camera; the camera does not see your network.

TECHNICAL SCOPE

Exposure audit

Which devices can be reached from the internet or the office, manufacturer P2P services and default passwords.

Segmentation

Separate networks for video, intrusion, access control, management and office, with explicit rules and a flow matrix.

Remote access

Over VPN only: no camera, recorder or panel exposed to the internet or dependent on the manufacturer's cloud services.

Power and continuity

Worst-case PoE budget, UPS and autonomy, and link redundancy where the risk requires it.

Hardening and lifecycle

Supported firmware, synchronised time so that evidence holds, event logging and verifiable configuration requirements.

WHEN TO CALL US

Cameras share the office network, you are about to allow remote access, nobody knows what is exposed to the internet, or the installation is about to grow.

WHAT YOU RECEIVE

Network architecture

Flow matrix

Configuration requirements

Test protocol

REFERENCE STANDARDS

IEEE 802.1Q	Virtual LANs (VLAN)
IEEE 802.1X	Port-based access control
IEEE 802.3at/bt	Power over Ethernet (PoE)
EN 62676	Video surveillance

NOT INCLUDED

Equipment supply, network configuration and operation, and ongoing supervision services.

DESIGNS

S3 Ingeniería

CONFIGURES AND INSTALLS

The licensed company or
integrator you choose

OPERATES

Your team