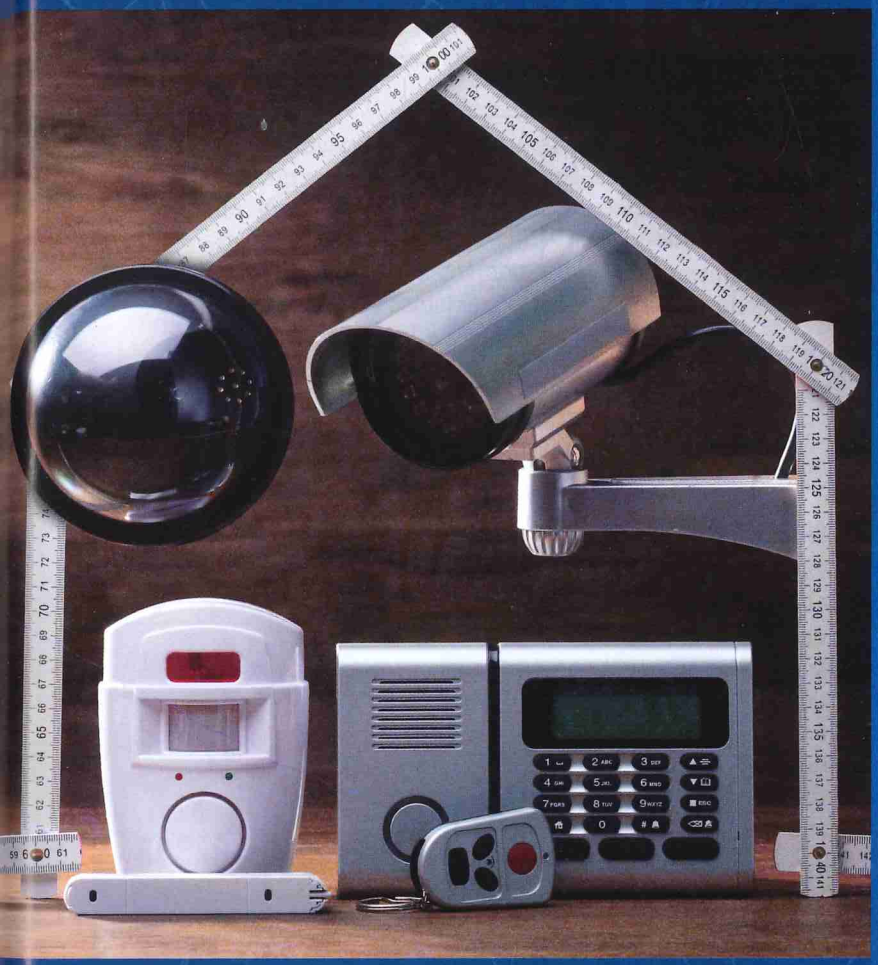
El área de seguridad

2



A partir de esta unidad, se comienza el estudio de las distintas áreas de las que se compone un hogar digital.

El estudio comienza por el área de seguridad, básica en las instalaciones de hogar digital, que permite un control local o remoto de las incidencias referentes a la seguridad del hogar.

En esta unidad se desglosarán los distintos tipos de instalaciones basándolos en la naturaleza propia de cada subinstalación de la red de seguridad. Hay que recordar que esta red forma parte de la infraestructura RGCS (red de gestión, control y seguridad) del hogar digital.

También se tendrá muy en cuenta la seguridad informática, debido a que un hogar digital está conectado a internet, de ahí que también aparezca un apartado expreso para ello.

Contenidos

Objetivos

- Conocer los elementos y las subinstalaciones en las que se divide el área de seguridad en el hogar digital.
- Reconocer los distintos tipos de instalaciones de seguridad para un hogar, así como su grado de seguridad según la escala.
- Determinar los servicios que el área de seguridad debe incluir para formar parte de un hogar digital.
- Clasificar los distintos tipos de elementos en función del tipo de seguridad que se desee obtener y aplicar en la instalación general.
- Reconocer fallos y avisos en los elementos que conforman la instalación.

2.1. La seguridad electrónica en el hogar digital

El área de seguridad electrónica en el hogar digital posee el objetivo primordial de realizar una protección del conjunto de la vivienda, los bienes del hogar donde están instalados y de las personas que se encuentran dentro de él de manera local o remota. Además, como un añadido a este objetivo, puede permitir así mismo la comunicación de lo que está ocurriendo al usuario o centro de control.

La composición de cualquier instalación de seguridad quedará completa con los elementos siguientes:

- **Elementos de detección.** Estos elementos se encargan de percibir mediante la lectura de magnitudes físicas (temperatura, presencia de energía IR, presión, etc.) el estado del lugar donde se encuentran instalados. Después devuelven una señal eléctrica a los elementos de control para el procesamiento. Estos elementos suelen ser los detectores y los sensores, que ya vimos en la unidad anterior que no eran lo mismo.
- **Elementos de control/gestión.** Estos elementos se concentran en la central de alarma, se encargan de gestionar las señales recibidas de los elementos de detección y poner en funcionamiento los elementos de actuación cuando sean necesarios y si la instalación está preparada para ello, comunicarse con una central receptora de alarmas (RCA o **CRA**), también llamada «central de monitoreo», que se encarga de controlar, gestionar y monitorizar de manera remota las señales emitidas por la central de alarma local. Dentro de estos elementos se encuentran también los paneles de control, que se encargan de permitir al usuario/técnico la configuración de la central local.
- **Elementos de actuación.** Son los encargados de avisar, modificar o subsanar en su caso, mediante los mecanismos oportunos, las incidencias aportadas por los elementos de detección. Son controlados por la central de alarma. Algunos ejemplos pueden ser: electroválvulas, gabinetes de sirena exterior, etcétera.

Una vez analizados los elementos, se deben observar los distintos niveles en los que se puede categorizar la seguridad electrónica. Dependiendo del tipo que sea, los elementos a utilizar variarán en cantidad, tipos, conexionado y calidad de servicio.

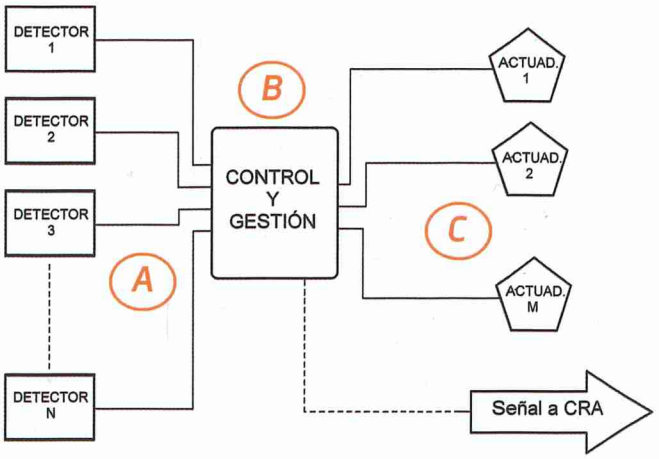


Figura 2.1. *Gráfico general de los elementos existentes en una instalación de seguridad. A. Elementos de detección; B. Elementos de control y gestión; C. Elementos de actuación.*

Recuerda:

En la unidad anterior, se explicó que un detector y un sensor no son lo mismo, dependen del tipo de respuesta que devuelve cada uno.

El detector dará una respuesta indicando que se cumple o no su condición de detección, por ejemplo si hay humo o no, si hay luz o no, etc. Su respuesta es una respuesta digital.

El sensor dará una respuesta indicando qué cantidad de magnitud detectada hay, por ejemplo qué cantidad de CO_2 existe, qué temperatura hace, etc. Su respuesta es una respuesta analógica.

Niveles de seguridad

La seguridad queda dividida normalmente en cinco niveles o grados dependiendo de los locales donde se vayan a ins-

Vocabulario

Energía IR: energía infrarroja, energía no visible ya que su longitud de onda se encuentra por debajo del espectro de luz visible, que se obtiene del calor que desprende un cuerpo.

Espectro de luz visible: el espectro de luz visible lo forman los colores que el ojo humano puede ver y que va desde el color rojo al violeta (arco iris). Este espectro se obtiene del reflejo de la luz blanca pura sobre los objetos y el color que el objeto devuelve reflejado hasta el ojo humano.

talar y de la preparación mínima que necesitaría cualquier intruso que desee acceder al hogar, salvo el grado 0, los demás están regidos por una normativa legal específica de cada país.

La graduación de niveles de seguridad queda especificada de la siguiente manera, según lo establecido en las normas UNE-EN:

- **Grado 0:** grado de seguridad **«muy bajo»,** se trata de elementos puramente disuasorios, sin conexión a ningún tipo de elemento de control o centralita. Ejemplos de este grado serían los avisos de «Cuidado con el perro», carteles de videograbación sin cámaras instaladas, carcasas de cámaras con luces simulando una grabación, un pitido al acceder a un local.

  No está incluido en la graduación de las normas UNE-EN, aunque se considera interesante reseñarlo.

  Cualquier intruso sin preparación técnica alguna podría realizar una incursión en nuestro hogar.

Figura 2.2. *Carteles de tipo disuasorio que se enmarcan en el grado 0 de seguridad.*

- **Grado 1:** grado de seguridad **«bajo»,** se trata de instalaciones básicas, realizadas en el hogar principalmente, con el control y la supervisión del usuario pero sin conexión a una CRA o empresa suministradora de servicios de seguridad.

  Cualquier intruso con preparación técnica básica, uso de polímetro y una herramienta básica, podría realizar una incursión en nuestro hogar.

- **Grado 2:** grado de seguridad **«medio»,** se trata de instalaciones de prevención de intrusión y CCTV básica, realizadas normalmente en hogares y pequeños establecimientos, que sí cuentan con conexión y supervisión de una CRA o empresa suministradora de servicios de seguridad.

  Los intrusos deben tener una preparación técnica, uso de polímetro y una herramienta básica, así como nociones de comunicación.

Figura 2.3. *Ejemplo de vivienda con sistema de seguridad y servicios necesarios para ser considerada de grado 2.*

- **Grado 3:** grado de seguridad **«medio-alto»,** esta graduación la recibirán los locales y establecimientos que en su día a día poseen movimiento de caudales o de objetos de alto valor. Por ley, desde este grado, están obligados a tener instalado un sistema de seguridad. Se utilizan elementos de seguridad y CCTV de una complejidad aceptable. Los sistemas se encuentran controlados y supervisados por un CRA o empresa de seguridad. Entrarían en este grado supermercados, joyerías, pequeños bancos, etcétera.

  El intruso debe poseer unos conocimientos altos en cuento a técnica y seguridad para poder realizar una intrusión en los locales de este grado de seguridad.

Figura 2.4. *Seguridad de grado 3 en un supermercado, debido a que es un establecimiento con movimientos económicos.*

- **Grado 4:** grado de seguridad **«alto-muy alto»,** máximo existente a nivel legal, este grado de seguridad se aplica a entidades y organizaciones de las cuales depende el bienestar general de la población. Hablamos de centrales de bancos nacionales, instalaciones militares, instalaciones gubernamentales o entidades internacionales.

  El intruso, como se puede sobreentender, debe ser experto en seguridad.

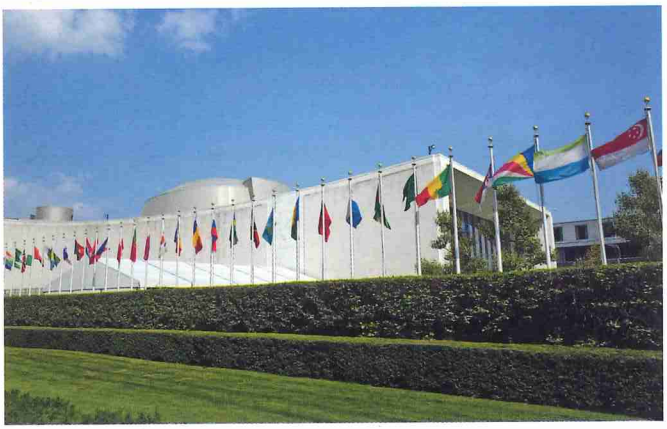


Figura 2.5. *La ONU es un ejemplo a gran escala de organizaciones que deben incorporar un sistema de seguridad de grado 4.*

Observando los datos detallados, se puede concluir que **cualquiera de las instalaciones que se vayan a desarrollar en el hogar digital estarán enmarcadas en el grado 2.**

Ahora, y como bien expone la titulación de este módulo formativo, *Hogar digital y sistemas integrados*, en las instalaciones de seguridad del hogar digital se trabaja por la integración, que hace ya tiempo se vio como una forma innovadora que permite realizar, bajo la gestión de un software, el monitoreo en tiempo real de todos los sistemas del hogar y, en concreto, en este caso, en el área de seguridad.

Toda esta integración en el hogar digital se consigue gracias a la pasarela residencial, que es el elemento integrador de todas las distintas redes de la instalación, también se puede realizar a través de equipos informáticos con software específico. A continuación, se muestran las ventajas de este tipo de trabajo:

- Elimina la necesidad de manejar cada sistema por separado, evitando así la **redundancia** o reduciéndola en su caso.
- Se reduce en gran medida el número de falsas alarmas ocasionadas por otros sistemas revisando los elementos que se encuentren bajo la cobertura de las cámaras de la protección con circuito cerrado de televisión (CCTV), logrando la confirmación visual de la alarma anunciada.
- El elemento o sistema que realiza la integración, en la mayoría de los casos, muestra un interfaz amigable y autónomo, donde las tareas preventivas son automáticas, «saben» cómo actuar ante cada contingencia, evitan las falsas alarmas, detectan problemas técnicos, etc., evitando de este modo las configuraciones iniciales al usuario final, que puede o no saber del tema en cuestión.
- El coste de mantenimiento se reduce, al no necesitar más que una sola plataforma que centralice todos los servicios.
- Permite el acceso remoto con la comunicación de internet básica basada en protocolos TCP/IP.

Vocabulario

Redundancia: consiste en realizar la misma labor repetidas veces, cuando sería necesario solamente una.

TCP/IP (*Transmission Control Protocol/Internet Protocol* o protocolo de control de transmisión/protocolo de internet): modo de comunicación informática que engloba una serie de normas y operaciones que permiten la comunicación mediante internet.

2.2. Legislación sobre seguridad

La legislación sobre las instalaciones de seguridad en el hogar digital se sustenta en la normativa existente sobre la instalación y el funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada. Cada país posee su legislación propia en este aspecto, en España se cuenta con una legislación específica en la Orden INT/316/2011, de 1 de febrero, del Ministerio del Interior. De esta orden ministerial, a continuación se realizará un breve resumen de los apartados más importantes tanto para el instalador como para el usuario de la instalación.

Sobre la instalación

Para realizar la conexión de aparatos, dispositivos o sistemas de seguridad privada a centrales de alarmas y CCTV (CRA, centro de registro de alarmas) será preciso que:

- La instalación haya sido efectuada por una empresa de seguridad inscrita en el registro correspondiente.
- El material que se instale y utilice se encuentre debidamente aprobado, según lo establecido en el artículo 3 de la Orden INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada.

- Se cuente con el pertinente certificado de instalación y que se lleven a cabo las revisiones preventivas, conforme a lo que determinan los artículos 4 y 5 de la mencionada Orden.
- Además de lo anterior, la instalación debe realizarse por personal acreditado y certificado en instalaciones de seguridad privada. Este puede coincidir con personal contratado por la empresa de seguridad, en cuyo caso, se da por supuesta esta certificación del instalador.

Funcionamiento y verificación

La atención a las centrales de alarma debe ser permanente, al menos dos operadores de la empresa suministradora del servicio de seguridad se harán cargo del buen funcionamiento de los receptores y la transmisión de las alarmas recibidas.

La verificación, una vez recibida una notificación de alarma, debe ser inmediata, utilizando los procedimientos técnicos y/o humanos que se indican a continuación:

- Verificación secuencial, deben activarse las alarmas con una determinada secuencia para considerar el aviso válido.
- Verificación por vídeo, cuando una alarma haya sido activada se activará la visualización a través de vídeo por medio de un detector de intrusión o un videosensor,
- Verificación mediante audio, se trata de la transmisión de una grabación de audio a la CRA justo antes de activarse la alarma y en el momento de la activación, también permite la transmisión de audio en directo.
- Verificación personal, la empresa suministradora del servicio de seguridad podrá personarse a comprobar la situación de alarma, siempre al amparo de miembros de las Fuerzas y Cuerpos de Seguridad del Estado.

Custodia de llaves

El servicio de custodia de llaves puede ser contratado con la empresa suministradora de la seguridad, de este modo, la empresa podrá personarse en las propias instalaciones (a este respecto, existe un artículo específico en la orden ministerial expuesta anteriormente).

Solo vigilantes de seguridad, con autorización expresa y escrita de los dueños del inmueble, podrán realizar la verificación personal e inspección del local donde esté la alarma, portarán las llaves para facilitar a las Fuerzas y Cuerpos de Seguridad del Estado la información necesaria sobre el posible delito cometido en el inmueble.

Las empresas de seguridad, para ofrecer este servicio, podrán contar con vigilantes de seguridad sin necesidad de estar inscritas y autorizadas para la actividad de vigilancia y protección de bienes, o bien subcontratar tal servicio con una empresa de esta especialidad.

Falsas alarmas

Cuando el sistema de seguridad origine dos o más falsas alarmas en el plazo de un mes, se pedirá, a través de las autoridades competentes, al titular de los bienes protegidos, para que en un tiempo máximo de 72 horas proceda a la subsanación de las deficiencias que dan lugar a las falsas alarmas, pudiendo acordar la suspensión del servicio, ordenando su desconexión o la obligación de silenciar las sirenas, por el tiempo que se estime conveniente.

Libros y registro

Las empresas de explotación de centrales de alarmas llevarán un libro-registro de alarmas, cuyo modelo se ajuste a las normas que apruebe el Ministerio del Interior, de forma que sea posible su tratamiento y archivo mecanizado e informatizado.

Las centrales de alarmas que tengan contratado servicio de custodia de llaves indicarán en el libro-registro de contratos cuáles de estos incluyen aquel servicio.

Con respecto a la custodia de las imágenes de sistemas de CCTV, deberán almacenarse un máximo de 30 días y estar a disposición de las Fuerzas y Cuerpos de Seguridad del Estado cuando sean requeridos para la comprobación de cualquier acto delictivo.

2.2.1. Ley general de protección de datos (RGPD)

La Ley general de protección de datos (GDPR, *General Data Protection Regulation*, o RGPD, Reglamento general de protección de datos de la UE) consiste en una serie de regulaciones que la Agencia española de protección de datos (AEPD), a través del Supervisor europeo de protección de datos (SEPD), ha confirmado como adecuadas en las garantías de los compromisos contractuales, brindados por Google para las transferencias internacionales de datos a América en general y en particular a Estados Unidos. Todo ello a través de las herramientas G Suite y Google Cloud Platform.

Se cumple así que las protecciones legales que sustentan todos los flujos de datos internacionales de estas herramientas cumplen al 100 % los requisitos.

Sabías que

El SEPD (Supervisor europeo de protección de datos) se encarga de supervisar, asesorar, tramitar las reclamaciones, colaborar con las autoridades de cada país y supervisar las nuevas tecnologías que pueden tener una incidencia en la protección de datos.

Este reglamento entró en vigor el 25 de mayo de 2018, y fue cuando reemplazó cualquier normativa de protección de datos vigente hasta el momento en los distintos países donde se aplica. Esto supone un gran avance, ya que:

- Unifica las normas de protección de datos en toda Europa.
- Fortalece los derechos de los ciudadanos de toda Europa.
- Establece nuevas obligaciones para todas las organizaciones que ofrecen bienes y servicios en línea.

Concretando, la RGPD logra con esta normativa que:

- Se asegure de manera fehaciente que los datos de los usuarios solo se utilizan para fines específicos.
- Los datos que se recopilan sean precisos y solo los indispensables.
- El almacenamiento de los datos se realice únicamente durante el tiempo que es necesario para el fin especificado.
- Se prevenga el uso no autorizado de los datos, su pérdida y filtración.

Todo esto se cumple gracias a que la norma obliga a las empresas a ser transparentes con los usuarios en cuanto a la manera, cómo y para qué, del uso de sus datos personales.

2.2.2. Ley general de protección de datos en los sistemas de videovigilancia

Es importante saber cómo se relaciona lo estudiado hasta el momento con la materia en estudio y es en este apartado donde se observa esta relación, ya que dentro de la seguridad del hogar digital aparecen los circuitos cerrados de televisión o instalaciones de videovigilancia, de los cuales hay un apartado explícito dentro de la RGPD.

A la hora de la realizar cualquier instalación de videovigilancia, hay que ser consciente que al realizar una grabación y almacenamiento de personas y lugares, la labor de la empresa instaladora o el instalador homologado está sujeta al cumplimento de la RGPD. La grabación de personas físicas conlleva implícitamente unos derechos de imagen que deben ser salvaguardados.

En primer lugar, la videovigilancia debe estar avisada de manera clara para aquellas personas que accedan al lugar en el que se está desarrollando la toma de imágenes, dando la libertad de no acceder al recinto.

Figura 2.6. *Distintos tipos de letreros informativos sobre la grabación de imágenes mediante un circuito cerrado de televisión.*

En segundo lugar, la instalación de seguridad debe estar **inscrita mediante un fichero** en el Registro general de protección de datos (RGPD) de la Agencia española de protección de datos. Una vez inscrita, debe ser legalizada como instalación de videovigilancia de carácter individual o de comunidad de vecinos.

Para que la legalización tenga validez, deberá contemplar los siguientes apartados mínimos:

- **Responsable del fichero.** Aquella persona física o jurídica responsable del fichero que decida sobre la finalidad, contenido y uso del fichero, normalmente es el propietario de la vivienda o la comunidad de vecinos en instalaciones comunitarias.
- **Derechos de oposición, acceso, rectificación y cancelación.** Deberá cumplimentarse en el caso de que la dirección donde se prevea atender al ciudadano que desee ejercitar sus derechos de oposición, acceso, rectificación y cancelación sea diferente a la del responsable del fichero.
- **Encargado del tratamiento.** Este apartado únicamente habrá de cumplimentarse cuando un tercero realiza el tratamiento por cuenta del responsable, e implique una ubicación del fichero distinta a la indicada en el responsable de fichero.

Un **ejemplo** de encargado de tratamiento de los datos para el caso de la videovigilancia podría ser el de las empresas de seguridad que prestan servicios combinados de central de alarmas y videovigilancia de modo que cuando se activa la alarma se comprueban directamente las imágenes por el personal de la empresa de seguridad. En cambio, la empresa instaladora del sistema de videovigilancia no implica en ningún momento el acceso a las imágenes y por tanto no tendría consideración de encargado del tratamiento.

- **Identificación y finalidad del fichero.** Como bien nos especifica la normativa de la RGPD, debe quedar bien definida la finalidad de los datos que se van a captar, así como dónde quedarán almacenados.

Recuerda:

Una instalación de videovigilancia, para estar acorde a la ley, debe:

- **Estar inscrita en el fichero** correspondiente en la Agencia española de protección de datos (AEPD).
- Debe informar con lo dispuesto en la LGPD, colocando distintivos con la información específica de los propietarios del fichero para dar a conocer la existencia de cámaras de videovigilancia.
- El técnico-instalador de manera obligatoria debe cumplimentar el **documento de seguridad** referente a la instalación de videovigilancia.
- No grabar o capturar imágenes de espacios públicos de no ser algo inevitable debido a su ubicación o que sea imprescindible para la finalidad de la grabación.
- No obtener imágenes de espacios íntimos, como por ejemplo aseos.
- Tomar medidas de seguridad respecto a la recogida de las imágenes y recuperación de las grabaciones. Por ejemplo, que la zona de almacenamiento de las imágenes no sea un espacio de público acceso.
- Almacenar las imágenes un tiempo máximo de **30 días.**
- Dejar a disposición judicial imágenes o grabaciones que contengan incidencias o delitos.

2.3. Infraestructura de seguridad. Medios de transmisión y tipos de instalaciones

Este apartado se centra en el estudio de las estructuras que se utilizarán para la conexión de todos los elementos que forman la red de seguridad y que a su vez se enmarca dentro de la red de gestión, control y seguridad del hogar digital (RGCS).

Se definirán las distintas vías y elementos de comunicación para una instalación completa de seguridad en el hogar digital, desde el control de acceso a la seguridad antirrobo, intrusión o incendio. A continuación, habrá elementos que aparezcan nombrados aunque no explicados, esto se debe a que este apartado se centra en la infraestructura. El estudio de los distintos elementos que compone este tipo de instalaciones se detalla en el apartado siguiente.

Las instalaciones, en primer lugar, se diferenciarán principalmente en el tipo de seguridad que se desee instalar, así se pueden encontrar instalaciones antiincendio, antiintrusión, de videovigilancia o CCTV, tal y como se va estudiando a lo largo de esta unidad.

Otra posible clasificación general se realiza dependiendo del tipo de conexión que realizan los detectores/sensores con la centralita de alarma, así nos encontraremos la siguiente clasificación general:

- **Instalaciones en lazo abierto:** normalmente en instalaciones antiincendio.
- **Instalaciones en lazo cerrado:** normalmente en instalaciones antiintrusión.

Por tanto, la red de seguridad se dividirá en pequeñas subredes, dependiendo de la utilidad que se desea obtener de cada una de ellas; así se podrá realizar una clasificación como la siguiente:

- **Subred de videoportero:** utilizará las líneas de conexión necesarias para unir el monitor o teléfono con la placa de calle, así como los elementos mecánicos de abrepuertas y los elementos eléctricos necesarios, como son el distribuidor que se encarga de ubicar la llamada en la vivienda elegida y transmitir la señal

Sabías que

La intercomunicación privada en las comunidades de vecinos está formada por los porteros y videoporteros automáticos, no estando estos regulados por el Reglamento de ICT. Pero, cuando hay cámaras, estas sí están sujetas a la legislación sobre protección de datos.

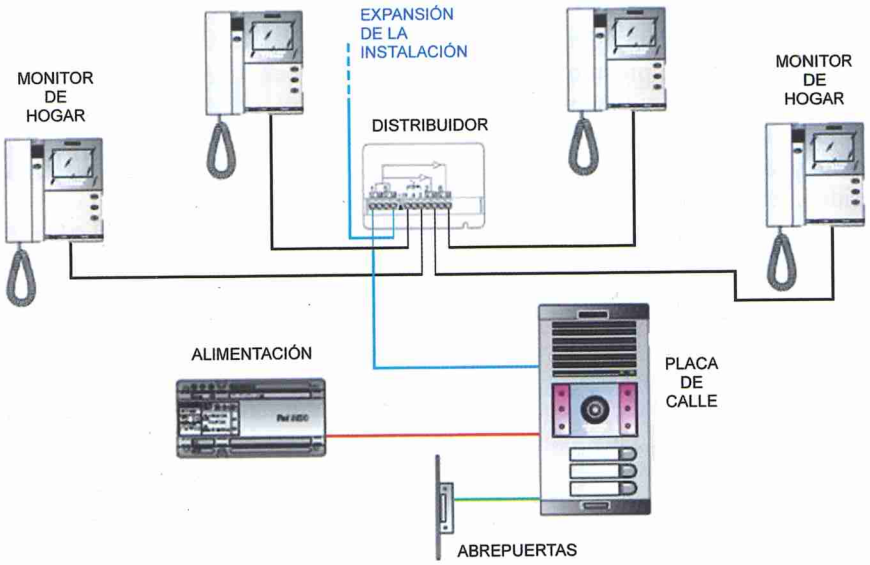


Figura 2.7. *Instalación tipo de videoporteros en una planta de cuatro viviendas de un edificio.*

de la cámara de la placa de calle y el alimentador que adapta la señal eléctrica general a la alimentación necesaria para los elementos de la instalación.

De manera general, para la comunicación utilizará cable de par trenzado con todos los hilos necesarios para la comunicación, para esto el par trenzado se categoriza dependiendo del número de pares que incluye en su interior, 2, 3, 4, 25 o 50 pares y del uso que se vaya a realizar. El tipo de cable utilizado dependerá si la instalación es residencial o individual.

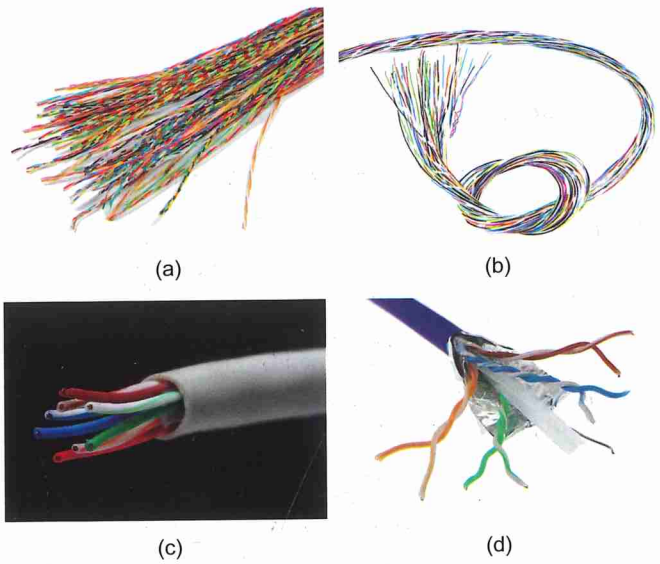


Figura 2.8. *Distintos tipos de cables de par trenzado: cable multipar de 50 pares (a), cable multipar de 25 pares (b), cable telefónico de cuatro pares (c) cable FTP de cuatro pares (d).*

Actividad propuesta 2.1

Tipos de instalaciones de videoportero

Estudiar las técnicas **4+N – Ningún dúplex, ADS y BUS2** de comunicación en instalaciones de videoporteros.

- Realizar un estudio de las tres técnicas, en cuanto a los medios y tipos de comunicación que realizan.
- Resumir las características propias de cada una de ellas, y realizar una especificación en características comunes y diferencias.
- Describir los elementos propios de cada una de las tecnologías.

Metodología:

- El trabajo se desarrollará de manera personal o en parejas.
- Presentar un documento con la información solicitada.

Sabías que

El cable de par trenzado de cuatro pares se puede encontrar en tres estándares de fabricación distintos:

- UTP (*Unshielded Twisted Pair*) o par trenzado no apantallado. Cable de pares sin protección electromagnética externa salvo la de la capa de PVC que la recubre.
- FTP (*Foiled Twisted Pair*) o par trenzado con pantalla global. Similar al cable UTP, pero posee un apantallado general que protege la información de ruidos electromagnéticos externos.

- STP (*Shielded Twisted Pair*) o par trenzado apantallado. Cada par lleva un apantallado propio, además todos los pares están recubiertos por una malla metálica que protege la información de todos los pares de ruidos electromagnéticos.

- **Subred antiincendio:** utilizará las líneas de conexión necesarias para unir los sensores (CO, CO_2, humo, etc.) y los pulsadores de pánico con la central de control; a su vez y dependiendo del tipo de instalación que sea, la central se conectará con los gabinetes de sirena exterior, elementos de extracción de gas, elementos de extinción automática y, llegado el caso, con la central receptora de alarmas y las Fuerzas y Cuerpos de Seguridad del Estado.

  El conexionado entre elementos, cuando la instalación es cableada, se realiza de manera general mediante cable telefónico de varios pares o cable UTP, salvo la conexión a la central de registro de alarmas que se realiza mediante cable telefónico o cable de red cat. 5 o superior. Cuando la instalación es inalámbrica, la comunicación se realiza mediante wifi o bluetooth, en este caso el punto de acceso es, o debe ser, la central de control que deberá ser administrada para realizar una conexión entre detectores y ella misma.

  Observando la Figura 2.9, hay que resaltar que el elemento de conexión al exterior será la pasarela residencial, o cualquier elemento que realice esa función en el hogar donde se ha instalado. También cabe destacar la zonificación de los elementos de detección, de este modo será mucho más intuitivo encontrar el incendio, además de resaltar que los elementos de actuación (ventilación, electroválvula de activación de los rociadores, gabinete de sirena, etc.) pueden o no estar instalados a la vez, de hecho es probable que en el mismo local sean incompatibles debido, sobre todo, a circunstancias eléctricas.

En cuanto a la tipología general, normalmente, las instalaciones antiincendio poseen una tipología de lazo abierto, ya que los sensores generan o favorecen el paso de pequeñas intensidades eléctricas (señales analógicas) o la existencia de pequeños voltajes que llegan a la central de alarma. Con estas señales, además de avisar de la existencia de un incendio, humo, exceso de temperatura, etc., son capaces de enviar a la central la cantidad exacta de la magnitud detectada.

Las instalaciones antiincendio, o de prevención y detección de incendios, realizan las siguientes funciones de manera ininterrumpida, ya que su diseño se centra en:

— Supervisar constantemente el estado de las instalaciones.

— Detectar el fuego en su estado inicial, e incluso, previamente a producirse la combustión.

— Localizar inmediata y puntualmente el foco que origina el fuego. Para esto será necesario una planificación clara a la hora de conectar los detectores a las distintas zonas para las que esté preparada nuestra central.

— Verificar las señales de alarma y transmitirlas.

— Activar equipos o sistemas para reducir el alcance del incendio.

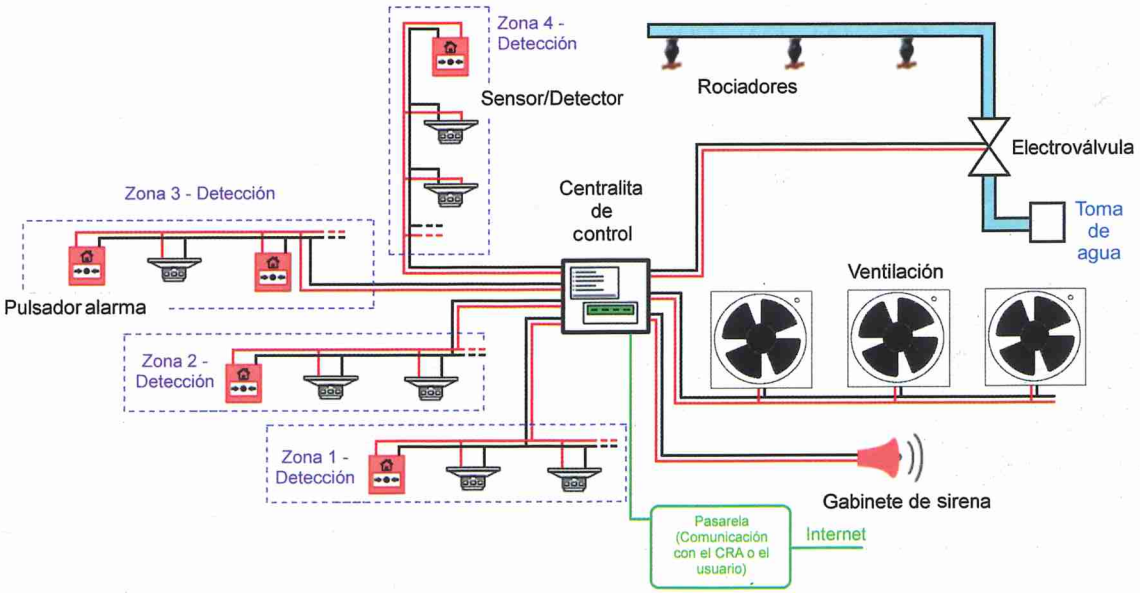


Figura 2.9. *Instalación completa tipo de un sistema de detección y extinción de incendios.*

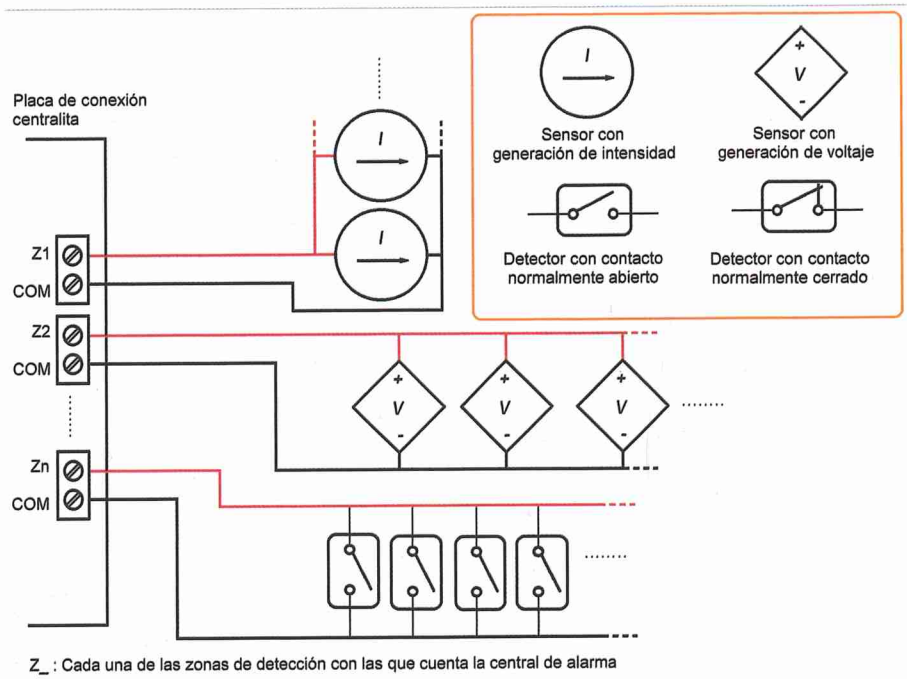


Figura 2.10. *Instalación genérica con conexión en lazo abierto. El número de zonas, detectores y/o sensores que se pueden instalar dependen del modelo concreto de centralita usada.*

- **Subred antiintrusión y robo:** utilizará las líneas de conexión necesarias para unir los detectores (infrarrojos, movimiento, apertura puerta, vibración, etc.) con la central de control. También puede contar (esto dependerá del tipo de comunicación de estos detectores) con una línea de vídeo adicional para los detectores que cuentan con una cámara incorporada, el funcionamiento normal de este tipo se realiza vía inalámbrica. Dependiendo del tipo de instalación, la central se conectará al gabinete de sirena exterior y a través de la pasarela, o el elemento que realice esta función, llegado el caso, con la central receptora de alarmas y las Fuerzas y Cuerpos de Seguridad del Estado.

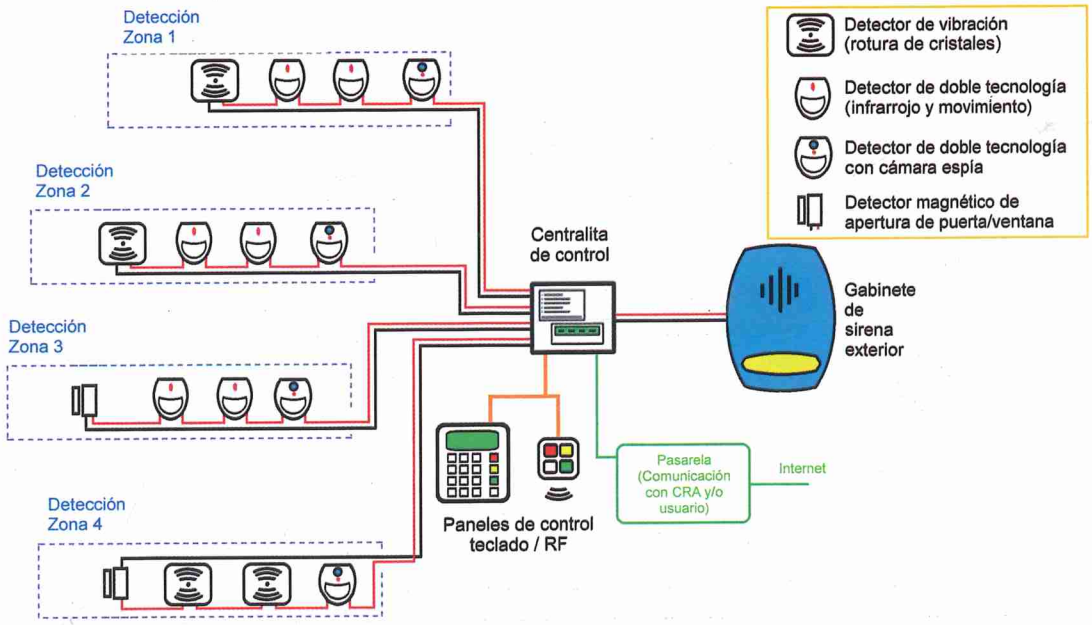


Figura 2.11. *Instalación tipo de un sistema de detección de intrusión y/o robo.*

El conexionado entre elementos, cuando la instalación es cableada, igual que en subredes anteriores, se realiza de manera general mediante cable telefónico de varios pares o cable UTP, salvo la conexión de la central de registro de alarmas que se realiza mediante cable telefónico o cable de red cat. 5 o superior. Cuando la instalación es inalámbrica, la comunicación se realiza mediante wifi o bluetooth directamente a la central o al panel de control, si van unidos en único elemento.

Las instalaciones antiintrusión cableadas, de manera general, y a diferencia de las antiincendio, poseen una estructura de lazo cerrado, es decir, que los detectores en este caso trabajan con sus contactos normalmente cerrados, propiciando así que la centralita se «autoenvíe» una señal de corriente por cada zona de detección. Cuando el detector se active, abrirá ese contacto y la señal dejará de llegar, informando a la centralita del estado de alerta.

Por norma general, una de las zonas, gracias a este tipo de montaje en lazo cerrado, se destina a la detección de los posibles sabotajes de los que pueden ser objetos los detectores.

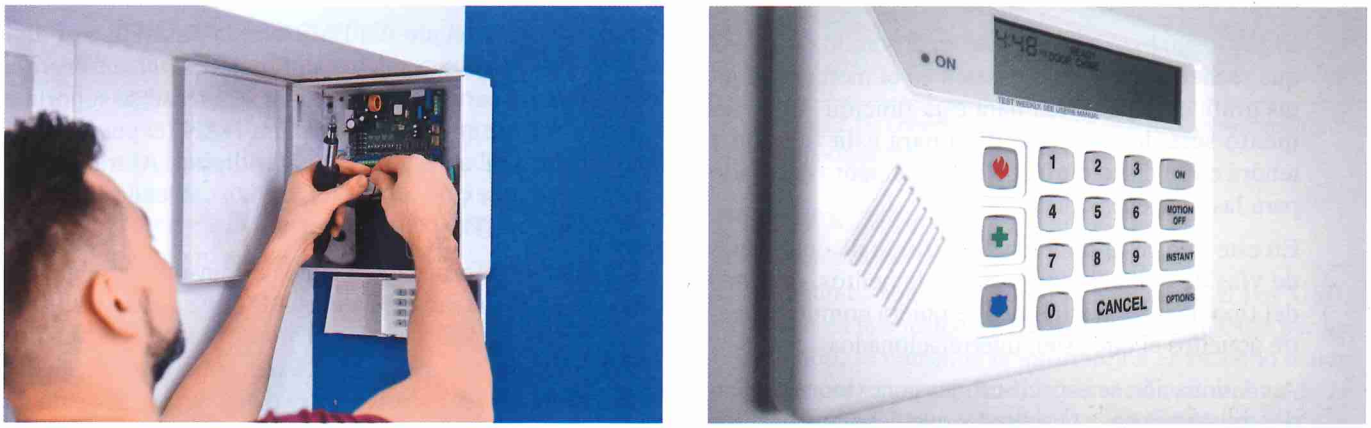


Figura 2.12. *Modelos distintos de central de procesamiento de señales de alarma. Izquierda, central cableada y panel de control externo. Derecha, central inalámbrica y panel de control integrados.*

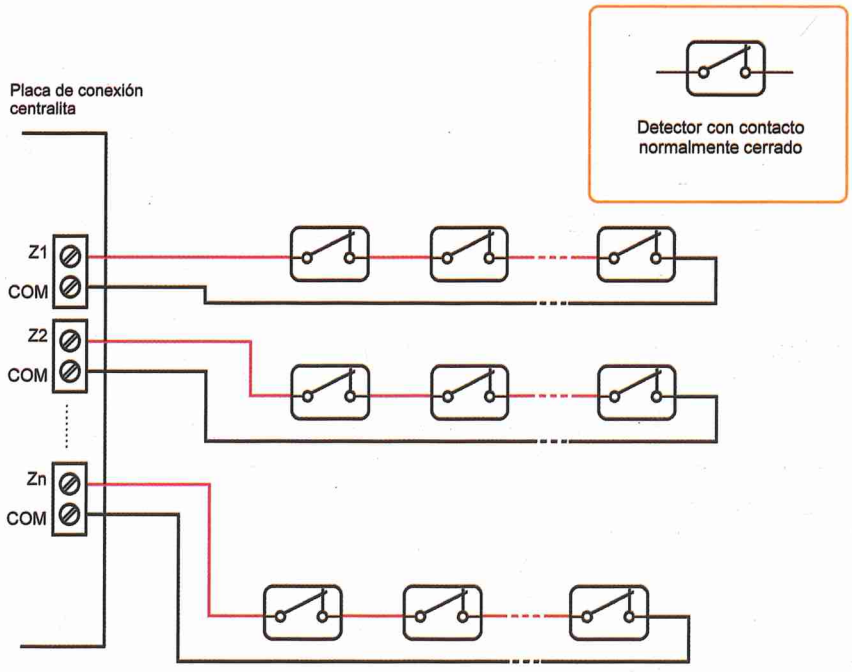


Figura 2.13. *Instalación genérica con conexión en lazo cerrado. El número de zonas, detectores y/o sensores que se pueden instalar depende del modelo concreto de centralita usada.*

- **Subred de videovigilancia (CCTV):** la subred de CCTV, a diferencia de las anteriores, no comunica señales eléctricas elementales desde las cámaras hasta el elemento de unificación de las imágenes (DVR, *Digital Video Recorder*), este envía a través de señales de vídeo compuesto las imágenes capturadas en directo por las cámaras. El conexionado es directo entre las cámaras y el DVR, este unifica las señales recibidas para proceder a su almacenamiento, local o remoto, y la comunicación, en su caso, con la empresa suministradora de los servicios, además de poder contar con un monitor para la visualización en directo de lo que ocurre en el área protegida.

  El DVR también puede estar incorporado en un PC que realice esta función, existen en el mercado tarjetas gráficas específicas para esta función. Este elemento será de uso específico para esta función y tendrá en su disco duro el almacenamiento necesario para las imágenes obtenidas.

  En este tipo de instalaciones, existirán distintos tipos de vías de comunicación entre elementos, depende del tipo de información que se quiera comunicar entre aquellos el que estén interrelacionados.

  A continuación se especifican las conexiones cableadas existentes en esta subred y que debemos tener en cuenta (Figura 2.14):

  — Conexionado de las cámaras con el DVR (*Digital Video Recorder*), *cableado marrón*, se trata de cables de vídeo (coaxial) o cables «siameses» (coaxial + alimentación). Si poseen también audio utilizarán un cableado aparte para ello, que se distribuirá junto con los citados anteriormente.

  — Conexionado del DVR con el monitor de visionado, *cableado naranja*, dependiendo del dispositivo de visionado se utilizará comunicación a través de cable VGA o si es de alta definición HDMI.

  — Conexionado del DVR con el dispositivo de almacenamiento, *cableado azul*, normalmente se tratará de cables de transmisión digital serie USB.

  — Conexionado del DVR con la pasarela o el dispositivo que realice su función, *cableado verde.* Esta parte de la subred de seguridad se soporta a su vez en la infraestructura HAN (expuesta en la unidad anterior) del hogar digital. Al tratarse de la conexión a internet, utiliza cableado UTP cat. 6 o STP.

  Toda la información recibida o transmitida se gestiona en la unidad de DVR o el PC en su caso dedicado a esta función, del mismo modo, todos los elementos protagonistas en esta subred irán conectados a este. En la Figura 2.15 se observa la placa de conexionado de un DVR genérico, en el que se observan conectores BNC, USB, RCA, VGA, RJ-45, HDMI, cada uno de ellos se utiliza para la conexión a un elemento diferente y realiza una transmisión de datos de distintos tipos.

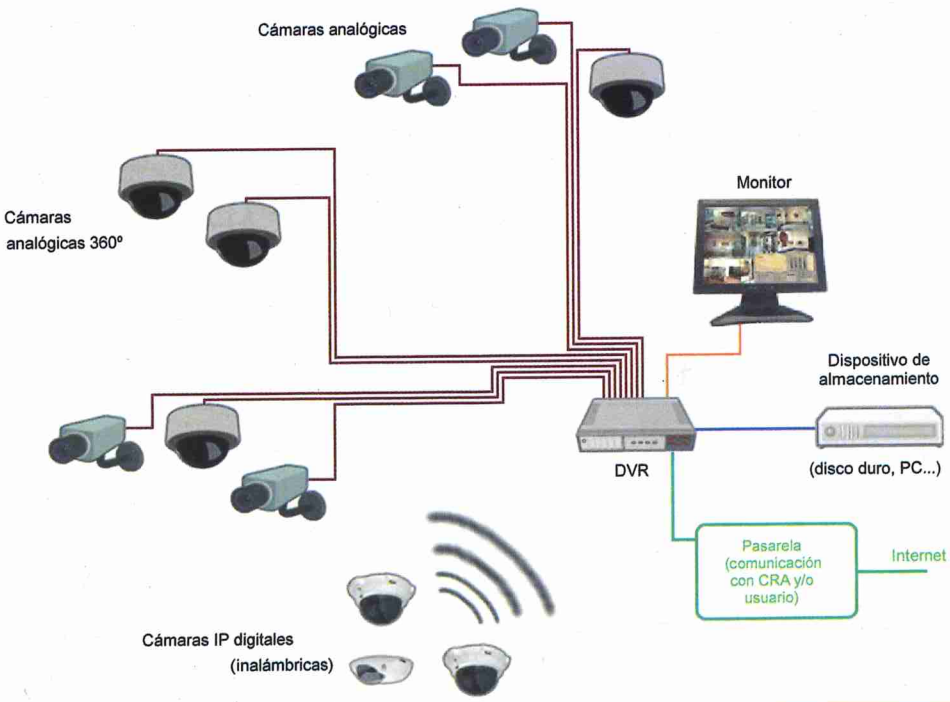


Figura 2.14. *Instalación básica tipo de los elementos de un CCTV.*

Figura 2.15. *Panel posterior de conexión de un dispositivo DVR genérico.*

Los estándares de conexión citados anteriormente son los siguientes:

— **BNC (*Bayonet Neill-Concelman*):** tipo de conector utilizado para cable coaxial. Usado por su seguridad de no poderse desconectar gracias a su «cierre por bayoneta». Se compone de un puntero que queda soldado al activo del cable coaxial y la estructura del conector que se conecta directamente a la malla mediante la sujeción por crimpado o roscado.

Figura 2.16. *Conectores de tipo BNC. Roscado, hembra y macho respectivamente.*

Para la conexión de las cámaras de seguridad, normalmente se utiliza el cable «siamés», cuya característica principal es que bajo el mismo aislante se unifican los hilos que componen el coaxial de transmisión de vídeo y los hilos necesarios para la alimentación de las cámaras.

— **USB (*Universal Serial Bus*):** se trata de un bus serie de comunicación digital. Su uso se ha generalizado tanto que ha generado un estándar de conexión para la transmisión de información por comunicación serie. Utiliza comunicación full-duplex.

El conector posee cuatro pestañas conductoras que conectan los cuatro hilos de los que se compone el cable. Dos de ellos son para la transmisión de la tensión de alimentación (los de los extremos) y los dos de la parte central son los que se utilizan para la transmisión (Tx) y recepción (Rx) de la información digital.

A su vez, este tipo de conectores se subdivide en seis tipos: USB-Type A, USB-Type B, USB-Mini A, USB-Mini B, USB-Micro A y USB-Micro B.

Figura 2.17. *Conectores de tipo USB-Type A. Hembra y macho, respectivamente.*

Sabías que

La comunicación serie, como la que utiliza el bus USB, consiste en la emisión y recepción de información por un único hilo, se transmite la información en bits uno detrás de otro por el mismo hilo, la recepción se realiza de la misma manera. La comunicación es posible gracias a la sincronización que se establece entre emisor y receptor. El tiempo de transmisión de cada bit de información es fijo, por tanto emisor y receptor, mediante el control de tiempo, son capaces de comunicarse.

Los tipos de comunicación serie son:

- **Full-duplex.** Puede transmitir y recibir simultáneamente. Utiliza dos líneas de comunicación, Tx para transmitir y Rx para recibir.
- **Half-duplex.** O solo transmite o solo recibe. Utiliza una sola línea de comunicación.
- **Simplex.** Solo se dedica a transmitir información binaria. Utiliza una única línea de comunicación.

— **RCA (*Radio Corporation of America*):** también llamado conector Cinch, su uso principal se centra en la transmisión de señales analógicas audiovisuales.

Se compone de un activo en el centro rodeado de una anillo metálico donde se conecta la masa, estos internamente se separan por una parte plástica para evitar errores por cortocircuito.

Necesita un único cable para cada señal a transmitir. Un ejemplo de su uso es para la transmisión de audio estéreo, utilizando dos cables, uno por cada canal.

Figura 2.18. *Conectores de tipo RCA hembras y machos.*

— **VGA (*Video Graphics Array*):** es un conector para la transmisión de la información producida por el estándar de vídeo que posee el mismo nombre. Su especificación forma parte de la norma o conjunto de normas conocidas como súper VGA.

Surge de la necesidad de centralizar en un circuito integrado los antiguos controladores de dispositivos de tubos de rayos catódicos y los sistemas que utilizaban.

Como resumen de características, posee una paleta de color de 262 144 colores distintos, con una definición máxima de 600 × 800 píxeles.

El cable que utiliza es propio del estándar compuesto por 16 hilos necesarios para la trasmisión de la información bajo este estándar.

Figura 2.19. *Conectores macho de tipo VGA (SVGA).*

Vocabulario

Píxel: es la menor unidad homogénea en color que forma parte de una imagen digital, dicho de otra manera más informal, es cada uno de los puntos luminosos de una pantalla de televisión, monitor o dispositivo de reproducción de imágenes que puede generar un color de la paleta de colores.

Paleta de colores: todos los colores diferentes que pueden ser tomados desde el rojo al violeta (colores visibles). Dependiendo de la definición del dispositivo esta agrupa desde los 16 colores básicos a los 224.

— **RJ-45:** conector que típicamente se utiliza para la comunicación por red Ethernet y acceso a internet mediante cableado estructurado. Se compone de 8 pines para realizar la conexión.

La conexión entre conectores RJ-45 se realiza mediante cable UTP, FTP o STP ya explicados con anterioridad en esta unidad.

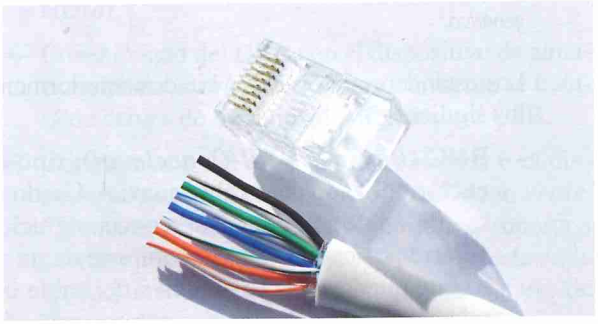


Figura 2.20. *Conector macho de tipo RJ-45 y cable FTP.*

— **HDMI (*High Definition Multimedia Interface*):** se trata del sustituto natural del euroconector para la adaptación a las imágenes y el vídeo de alta definición.

Es un conector con interfaz propia para la conexión de cualquier fuente de vídeo y audio digital, permitiendo el uso de vídeo digital de alta definición y de audio multicanal (hasta 8) en un único medio de transmisión.

A su vez, este tipo de conectores se subdivide en tres tipos: tipo A estándar normal, tipo C estándar mini HDMI y tipo D estándar micro HDMI.

Figura 2.21. *Conectores de tipo HDMI. Uno de tipo hembra y dos de tipo macho.*

— **Cable Ethernet PoE (*Power on Ethernet*):** se trata de un cable Ethernet (par trenzado) utilizado para la conexión de las cámaras IP cableadas, que utiliza las líneas que no reciben uso de trans-

misión de información para enviar la alimentación de los elementos a través del cable.

Las ventajas que ofrece este tipo de cable son las siguientes:

- ✓ Reduce los costes de instalación o ampliación en las redes de los edificios, evitando instalar nuevas líneas eléctricas que resultaría caro y complicado.
- ✓ Reduce los cables y las tomas de conexión necesarios.
- ✓ Permite utilizar un solo cable para todo.
- ✓ Permite llevar alimentación a lugares donde llevar tomas de alimentación es complicado, por ejemplo dobles techos.

Actividad propuesta 2.2

Resumen de las instalaciones de seguridad

Utilizando las herramientas gratuitas que nos ofrece la plataforma **genial.ly,** crear un «mapa mental» que resuma las características principales de las instalaciones que compondrán un área de seguridad de un hogar digital.

Metodología:

- Trabajo individual o por parejas.
- Una vez completada la actividad, realizar una presentación en clase con los resultados obtenidos.

2.4. Elementos de instalaciones de seguridad electrónica

Este apartado se centra en el estudio de los distintos elementos que compondrán una instalación de seguridad de manera general. Estarán por tanto definidos los elementos de instalaciones antiincendio y antiintrusión o robo. Estará bien observar de nuevo las Figuras 2.9 y 2.11 para centrar las ideas.

Para una mejor comprensión, se han separado en apartados distintos los elementos dependiendo de la subred a la que pertenecen, de este modo los elementos de CCTV y de control de acceso se estudiarán en apartados posteriores.

2.4.1. Elementos de detección

Los elementos de detección, de manera general, se encargan de percibir el estado del lugar donde se encuentran instalados y enviar las señales oportunas a las centrales para comunicar este estado. Podremos diferenciarlos en función de la característica que desean percibir.

Cuentan con una serie de características técnicas, que permitirán tomar la mejor decisión a la hora de utilizar unos u otros. Estas características son:

- **Rango de medida:** dominio en la magnitud medida en el que puede aplicarse el sensor.
- **Precisión:** es el error de medida máximo esperado.
- **Offset o desviación de cero:** valor de la variable de salida cuando la variable de entrada es nula. Si el rango de medida no llega a valores nulos de la variable de entrada, habitualmente se establece otro punto de referencia para definir el offset.
- **Sensibilidad de un sensor:** mínima cantidad de magnitud de entrada que el sensor es capaz de medir.
- **Resolución:** mínima variación de la magnitud de entrada que puede apreciarse a la salida.
- **Rapidez de respuesta:** puede ser un tiempo fijo o depender de cuánto varíe la magnitud a medir. Depende de la capacidad del sistema para seguir las variaciones de la magnitud de entrada.
- **Derivas:** son otras magnitudes, aparte de la medida como magnitud de entrada, que influyen en la variable de salida. Por ejemplo, pueden ser condiciones ambientales, como la humedad, la temperatura u otras como el envejecimiento (oxidación, desgaste, etc.) del sensor.
- **Repetitividad:** error esperado al repetir varias veces la misma medida.

Estas características son comunes y mínimas para todos los tipos de sensores, aunque en sensores más complejos pueden ampliarse.

De manera general, existen dos grandes subgrupos de sensores, estos dependen de la naturaleza de la señal generada:

- **Sensores pasivos:** son aquellos que generan señales y necesitan para ello de una fuente energética externa. Ejemplos: resistencias variables, de capacidad variable, de inductancia variable, etcétera.
- **Sensores activos o generadores de señal:** son aquellos que generan señales de forma autónoma, sin requerir de fuente alguna de alimentación. Ejemplo: sensores piezoeléctricos, fotovoltaicos, termoeléctricos, electroquímicos o magnetoeléctricos.

En los siguientes subapartados se irán detallando los distintos tipos de sensores y/o detectores que se instalan en estas estructuras, así como sus funcionamientos.

Sensores de incendios y gases

Son sensores capaces de percibir los efectos que produce un incendio. Se dividirán a su vez en:

- **Sensores de humo:** dispositivos capaces de detectar la presencia del humo producido por una combustión. Su funcionamiento se basa en la observación de la cantidad de micropartículas de ceniza existentes en el ambiente, para ello utiliza en su interior un emisor-receptor de infrarrojos (IR) que detecta cuándo se interrumpe la transmisión existente entre ellos.

  El receptor IR, de manera general, convierte en una señal de corriente la señal infrarroja que percibe.

Figura 2.22. *Sensor de humo.*

- **Sensores de gas:** dispositivos capaces de detectar la presencia de diferentes tipos de gases, normalmente no visibles al ojo humano. Su funcionamiento, a diferencia del anterior, se basa en la reacción. Internamente están compuestos por una o varias membranas que reaccionan al contacto con ciertos gases, estas membranas tienen una capacidad conductora en función del gas con el que se encuentran, de manera que al contacto con el gas concreto se vuelve más o menos conductora de la corriente eléctrica.

  Podremos encontrar sensores para gases como el CO_2, CO, butano, metano, propano, etc., que podrán detectar la presencia de un único gas o, en algunos casos, funcionarán de manera combinada como los sensores del gas natural.

Detectores de intrusión y robo

Son detectores que observan la posibilidad de la existencia de personas indebidas dentro del hogar o control de los medios de acceso al mismo. Dependiendo de la tecnología que utilizan, ofrecerán una funcionalidad distinta.

Figura 2.23. *Dos ejemplos de detectores antiintrusión. Arriba, detectores PIR por infrarrojos. Abajo, detectores magnéticos de apertura de puertas.*

A continuación, se presenta una breve clasificación de los detectores más generales que podemos encontrar, así como su funcionamiento y la funcionalidad para la que están preparados:

- **Detectores magnéticos:** son detectores formados por un imán y un contacto muy sensible a la variación magnética. El contacto estará cerrado o abierto, dependiendo del detector, al estar junto al imán, al separarse cambiará este estado. Estos detectores suelen instalarse en puertas y ventanas para detectar cuando son abiertas.
- **Detectores PIR:** detectores de movimiento por detección de energía infrarroja en el lugar y cambios de temperatura. De manera general, internamente mantienen una matriz que percibe energía infrarroja. Creando un mapa inicial, compara si la energía infrarroja sigue estando en las mismas celdas de la matriz y cuando existe un cambio en esta configuración se activa. Existen detectores PIR controlados para evitar la detección de mascotas.
- **Detectores termovelocimétricos (lapas):** se trata de detectores que van adosados al objeto a proteger, por ejemplo una caja fuerte, de ahí su nombre. Interna-

mente, incorporan tres tipos de detectores en serie: térmico, sísmico y de movimiento. De este modo, son capaces de detectar vibraciones, cambios de temperatura y movimientos del objeto que los aloja.

- **Detectores de inerciales o sísmicos:** detectan golpes o movimientos bruscos gracias a los mecanismos internos que poseen. De manera general, realizan la detección gracias a pequeños péndulos incorporados en su interior o pequeñas ampollas con mercurio. En ambos casos, el movimiento hace que, mediante el péndulo o el mercurio, se cierren los contactos que llevan internamente. Existe una gama bastante amplia donde elegir, los últimos modelos incorporan pequeños microprocesadores para su funcionamiento.
- **Detectores de ultrasonido:** detectores basados en la vibración provocada por sonidos de altas frecuencias. Usados normalmente para la detección de roturas en cristales, gracias a la detección del sonido que esta acción genera.
- **Barreras infrarrojas:** estos detectores necesitan de dos elementos, el emisor y el receptor de la señal infrarroja. Se basan en la detección de la ruptura del haz fotoeléctrico que se genera entre emisor y receptor. Su uso se centra en el control de acceso a zonas abiertas o el control de puertas con cierre automático para evitar accidentes.

En otro sector de la seguridad, podemos encontrar detectores como el siguiente, utilizado para la seguridad de personas solas:

- **Detectores de personas caídas:** detectores inalámbricos que permiten detectar desvanecimientos o caídas de personas que viven solas en su vivienda. También llamado «detector de hombre muerto».

2.4.2. Centralitas y paneles de control

Se trata de los elementos que forman el cerebro del sistema de seguridad electrónica, a ellos irán conectados todos los elementos de detección (Figuras 2.9 y 2.11). Dependiendo del tipo y modelo, ambos elementos pueden ir incorporados en el mismo bloque de la instalación o pueden aparecer por separado, de manera que la central se encontrará en un lugar protegido y el panel de control en un lugar más accesible al usuario (normalmente esto ocurre en instalaciones con sistemas cableados).

Se encargan, gracias a su programación, de la activación de los actuadores, de los elementos de aviso, así como de enviar la información a los CRA (centro de registro de alarmas) y las empresas que suministran los sistemas de seguridad.

Figura 2.24. *Centralita de alarma inalámbrica con panel de control incorporado.*

Se destacan en ellos las siguientes características:

- Admiten varios formatos de comunicación.
- Pueden ser controlados desde uno o varios teclados.
- Controlan varias zonas y permiten la posibilidad de expandir estas a más zonas.
- Poseen un *buffer* de almacenamiento de los eventos ocurridos.
- Permiten la movilidad y el control de detectores motorizados dándoles direccionabilidad.
- Pueden ser programados de manera remota (si están conectados a internet) o local.
- Pueden programar y controlar dispositivos externos a través de salidas programables.
- Pueden integrarse con sistemas de CCTV y control de acceso, atributo sin el cual no estaría completo el sentido de esta área en el hogar digital.

Actividad propuesta 2.3

Comunicación de centralitas

Estudiar los distintos formatos de comunicación que usan los sistemas de centralitas. Utilizando la herramienta online gratuita Kahoot, crear un juego para poner a prueba los conocimientos del resto de compañeros del grupo.

Metodología:

- Trabajo en grupos de 3-4 alumnos.
- Una vez realizada la actividad, dedicar una clase para que cada grupo ponga a prueba a los demás mediante el juego pedagógico creado.
- Para el docente puede utilizarse como prueba puntuable.

2.4.3. Actuadores

Son los elementos que realizan las acciones correctivas cuando la centralita detecta que existe un evento. Podremos encontrar:

- **Electroválvulas:** elementos mecánicos de control de flujo de líquidos o gases en la vivienda controlados eléctricamente.
- **Ventiladores:** utilizados para la extracción de gases o humos en espacios cerrados.
- **Indicadores luminosos:** utilizados para evitar la pérdida total de luz ante un momento de alerta.
- **Elementos de motorización:** son elementos mecánicos que se encargan de abrir ventanas o bloquear puertas; por ejemplo, motores, relés, pistones, etcétera.

2.4.4. Gabinetes de sirena exterior

Elementos de aviso externo controlados por la centralita. Se trata de los elementos instalados en el exterior del lugar protegido para generar avisos luminosos o sonoros de manera que llamen la atención ante cualquier evento que viole la seguridad del lugar.

Pueden contener circuitería para detectar en ellos mismos cualquier tipo de sabotaje, dando aviso de este mismo a la centralita.

Figura 2.25. *Gabinetes de sirena exterior.*

2.5. Instalaciones de control de acceso. Videoporteros

Esta parte de la red RGCS se encarga de controlar los permisos y las personas que podrán acceder a nuestro hogar, así como las tecnologías y los elementos utilizados para esta funcionalidad. Se incorporan a la red del videoportero (Figura 2.7), conectando los elementos de control de acceso a la placa de calle que se encarga a su vez del control del elemento para abrir la puerta.

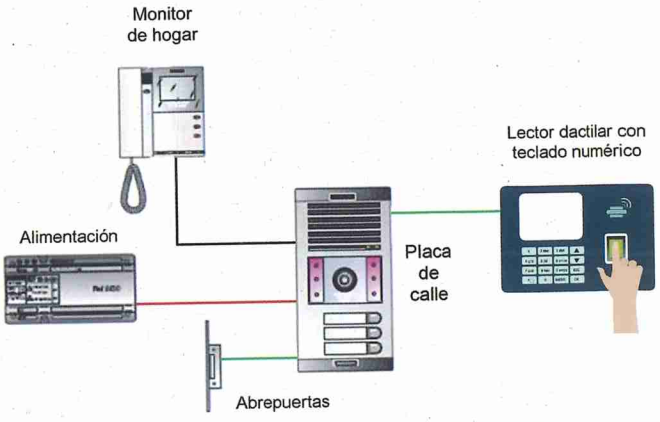


Figura 2.26. *Ejemplo de red de control de acceso con elemento híbrido o mixto.*

2.5.1. Elementos de lectura de información

En este apartado se estudiarán los elementos que utilizan las instalaciones de control de acceso para la lectura de información de la persona que desea acceder, de este modo se discriminará a aquellas que no posean los elementos de acceso o la información oportuna para conseguirlo.

Teclados numéricos

Se trata del elemento de control de acceso más básico y sencillo de todos los que se expondrán en este apartado. Al recibir una clave numérica introducida por el usuario, esta se comprobará en el dispositivo donde esté almacenada la clave y se procederá a su comprobación.

Sensores biométricos

Por todos es ya sabido que el cuerpo humano posee algunas características que hacen único a su portador, es por esto que en la seguridad aparecen también los elementos que son capaces de leer estas características únicas y utilizarlas como elemento de reconocimiento. También pueden ser combinados con elementos de reconocimiento del comportamiento para identificar de manera unívoca y verificable a la persona.

Tienen un uso preferencial como elementos de control de acceso a lugares, o control de permiso para usos de sistemas.

A continuación, se detallarán algunos de ellos, los que en el área que nos movemos suelen ser más utilizados. En todos

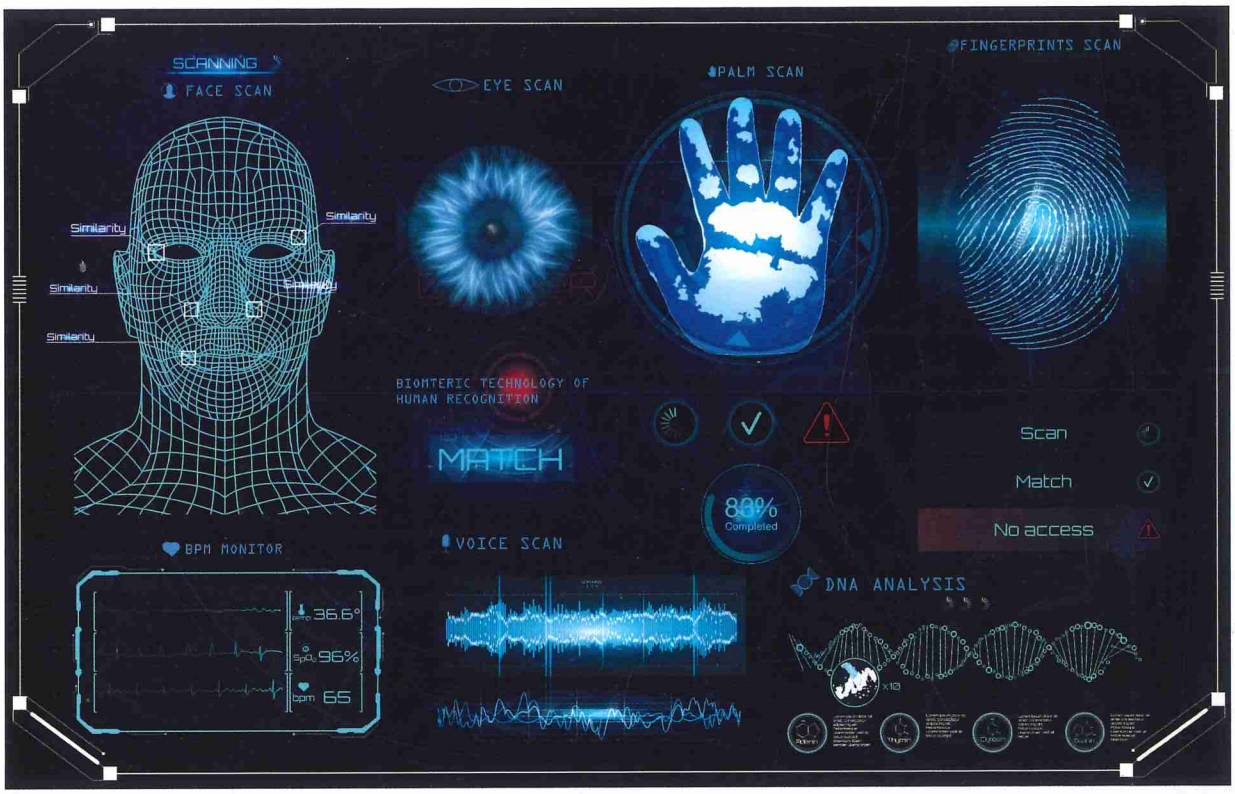


Figura 2.27. *Distintos tipos de detectores biométricos: facial, de iris, palmar, de huella dactilar, ritmo cardíaco, escáner de voz, analizador de ADN.*

ellos, lo que se realiza es una comparación entre los datos que se leen mediante el sensor y los que tiene almacenados en una base de datos de las personas que tienen acceso.

- **Lector de huella dactilar:** realiza una lectura mediante una pieza sensible al tacto de los pequeños surcos que existen en nuestros dedos y la convierte en una señal digital. De manera general suelen usarse los dedos pulgar e índice para este reconocimiento.
- **Lector de iris:** reconoce el tamaño del iris, los distintos colores que lo componen así como aspectos de la morfología del mismo. En la Figura 2.28 se puede observar la cantidad de información que un iris humano aporta, desde formas dibujadas hasta distintos colores en diferentes puntos.

Figura 2.28. *Iris de un ojo humano.*

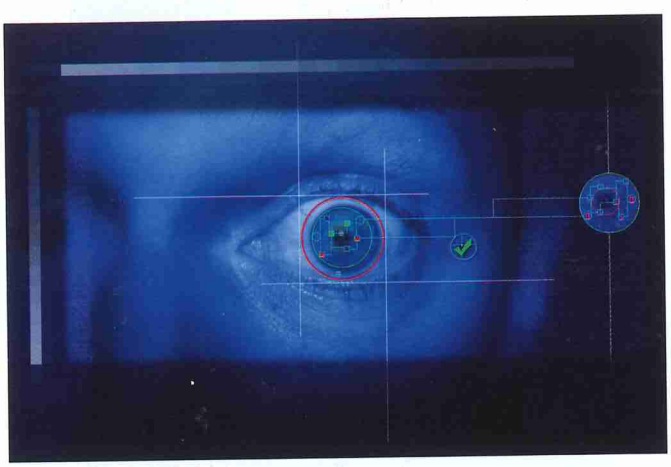
- **Lector de retina:** raras veces este lector se encuentra solo sin combinar con el anterior, lector de iris. Mediante un pequeño haz de luz, procede a la medición de la profundidad de la retina.
- **Lector palmar o plantar:** se basa en la medición de ciertos parámetros únicos de la palma de la mano o de la planta del pie. Parámetros típicos que suele tener en cuenta son las longitudes de palma o planta, la distancia entre la base de la mano y el dedo corazón, combinando reconocimiento de huellas dactilares y reconocimiento de la forma de las líneas de la mano (o el pie en su caso).
- **Reconocimiento facial:** se basa en la lectura de ciertos parámetros del rostro, como son: distancia ocular, forma de la cabeza, distancia entre orejas, posición de la nariz o distancia entre las comisuras de los labios, entre otras.

  Ya comienzan a utilizarse sistemas que incorporan sistemas 3D de observación y obtención de datos, añadiendo así a los anteriores más patrones para el reconocimiento.
- **Reconocimiento de voz:** la voz, una vez tratada eléctricamente, genera una señal analógica con parámetros medibles, como son la amplitud y la frecuencia, entre otros. Este sensor utiliza una frase de seguridad

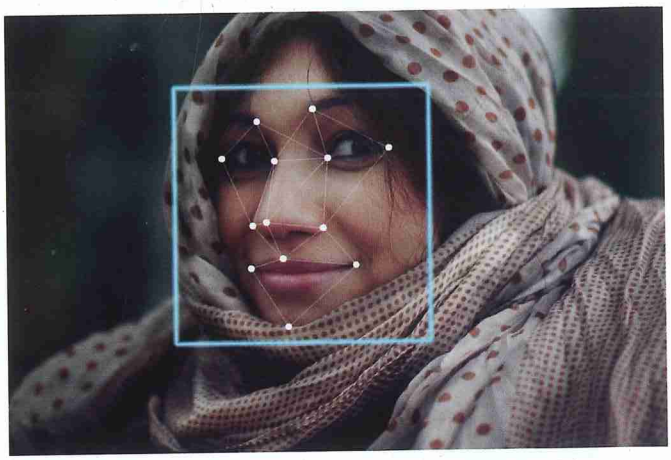
grabada, o bien una seriación de palabras, que quien desea realizar el acceso conoce.

El sensor realiza primero la función de transductor, para convertir la señal audible en una señal eléctrica, con la cual realiza una comparación de frecuencia, amplitud, etc., y dará la validez o no del acceso.

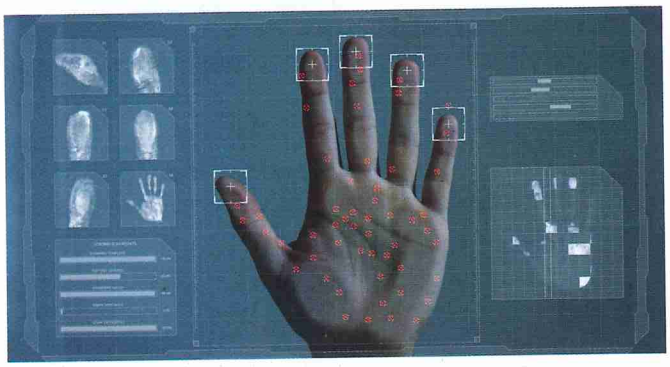
- Otros detectores más sofisticados destinados para sistemas de alta seguridad serían, por ejemplo, los **analizadores de ADN.** Estos, extraen algún patrón concreto del ADN de quien desea acceder y lo coteja con el banco de información con el que el sistema cuenta.



(a)



(b)



(c)

(d)

Figura 2.29. *Distintos parámetros de lectura biométrica: lectura de iris (a), lectura facial (b), lectura palmar (c), lectura dactilar (d).*

Actividad propuesta 2.4

Profundización en los sensores biométricos

Estudiar individualmente en otras fuentes (textos, investigaciones, internet, etc.) sobre los procedimientos concretos que utilizan los distintos sensores biométricos citados para realizar las autentificaciones.

Sacar conclusiones en pequeños grupos en clase y detallar cuáles son más idóneos para el objetivo de este módulo formativo.

Metodología:

- Realizar un resumen de los datos obtenidos.
- Exponer los resultados por grupos en clase (cuatro miembros como máximo).
- Hacer un informe final para entregar con las conclusiones y los datos obtenidos del debate en grupo.

Lectores de tarjeta

Los lectores son dispositivos utilizados generalmente para el control de acceso, su funcionalidad principal, como su propio nombre indica, es leer códigos generados por dispositivos externos y que portan solo las personas que tienen acceso al hogar donde se instala el sistema.

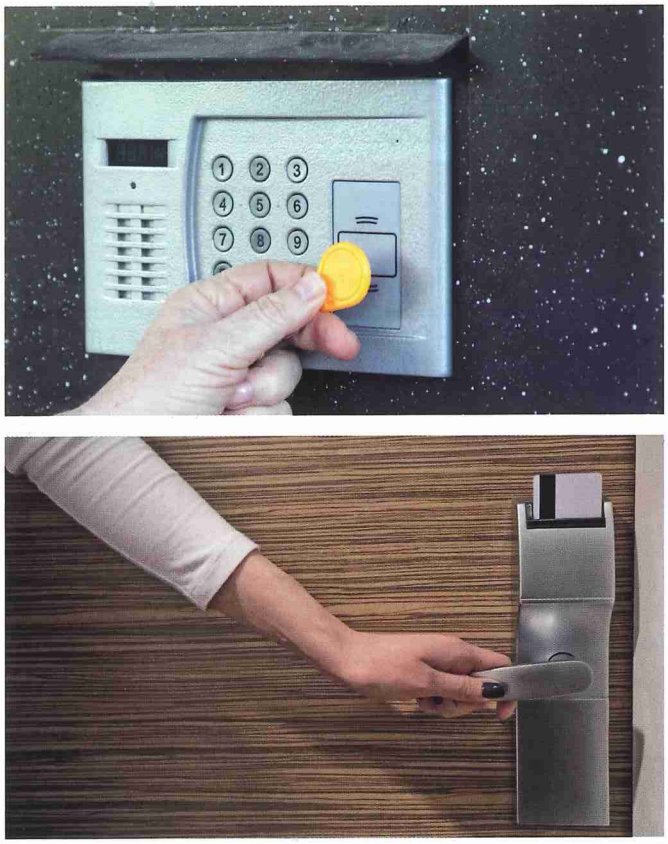


Figura 2.30. *Lectores de control de acceso: lector RFID (arriba) y lector de tarjetas con banda magnética (abajo).*

Existe una amplia variedad de dispositivos y fabricantes que se basan en las cinco tecnologías más extendidas y que se detallan a continuación, aunque de manera general son los de radiofrecuencia los más utilizados, quizá por su sencillez y precios más asequibles. Actualmente existen proyectos de nuevas tecnologías basadas en bluetooth que se comienzan a desarrollar.

A continuación, se muestran las tecnologías más utilizadas y que asumen los lectores usados para el control de acceso y la seguridad:

- **RFID (*Radio Frequency Identification*):** dispositivos con identificación por radiofrecuencia. Los datos son registrados en el chip que el dispositivo móvil tiene y no requiere contacto físico con el lector. Son ideales para los controles de acceso y de presencia.

  Se trata de un sistema de almacenamiento y recuperación de información almacenada de manera remota, con una lectura mediante ondas de radio.

  Los dispositivos móviles (tarjetas, etiquetas o transpondedores) incluyen una pequeña antena para responder ante las posibles peticiones de lectores de RFID.

  Son omnidireccionales, es decir, no hay que ponerlas en una dirección concreta para su lectura.

- **NFC (*Near Field Communication*):** dispositivos de comunicación en campo cercano. Funcionan mediante inducción de campos magnéticos que se obtienen gracias a las antenas en espiral que poseen las tarjetas móviles de esta tecnología.

  Esta tecnología comienza a ser utilizada en otros dispositivos móviles, teléfonos y tabletas, unida al bluetooth de los mismos.

- **Con chip:** utilizadas por tarjetas inteligentes, tarjetas chip o *smartcard*, los datos son registrados en el chip (de memoria o microprocesador).

  Algunos chips de memoria presentan un medio de codificación y de protección de escritura y es necesaria la inserción física de las tarjetas para su lectura en los lectores, aunque ya están comercializados sistemas híbridos que permiten la lectura sin contacto, por ejemplo, las tarjetas bancarias con Contactless. Son ideales para firma digital y control de acceso lógico.

- **Tarjeta con banda magnética:** todos los datos del usuario de la tarjeta se encuentran registrados en la banda magnética que hay incorporada en la tarjeta, permite la modificación de los mismos y da la posibilidad de poder personalizar los datos a almacenar.

  No permiten la lectura a distancia, es necesario un lector donde insertar las tarjetas debido a que la lectura se realiza por contacto físico.

- **Tarjeta con código de barras o códigos QR:** estas son las menos usadas por la facilidad de copia del código de barras impreso o el código QR, ya que este último es la evolución del primero.

  La información que contiene el código encriptado de manera gráfica será la encargada, una vez leída, de dar el acceso mediante el lector.

- **Chip subcutáneo:** es una aplicación que en los últimos años va ganando adeptos, se trata de un chip del tamaño de un grano de arroz con un transpondedor que almacena un código único, que se lleva bajo la piel. Utiliza tecnologías RFID o NFC para el reconocimiento a distancia. Como el código es único, permite la identificación unívoca de la persona que lo lleva implantado.

Vocabulario

Transpondedor: también llamado *transponder* en según qué ámbito tecnológico se utilice, se trata de un dispositivo de telecomunicaciones que posee la posibilidad funcional de «transmitir» y «responder», es decir, busca con quién comunicarse y, una vez establecida la comunicación, responde a las solicitudes de información que se le solicita.

Código de barras: código basado en la representación de barras de distintos grosores y espaciados, estos grosores y espaciados contienen una información en pequeñas cadenas de caracteres.

Código QR: codificación que mejora el código de barras, se representa de manera matricial a base de puntos. Los cuadros que posee en tres esquinas sirven para el posicionamiento del lector.

Tabla 2.1. Comparativa de las características de las distintas tecnologías

Características por tecnologías					
Áreas	RFID	NFC	Con chip	Banda magnética	Códigos de barras y QR
Nivel de seguridad	Medio-alto	Medio-alto	Alto	Medio	Bajo
Distancia de lectura del lector	10 a 100 m	< 20 cm	0 - Contacto	0 - Contacto	7,5 cm a 3 m
Frecuencia de transmisión	2,4 GHz	13,56 MHz	–	–	–

Grupal

Actividad propuesta 2.5

Estudio de las distintas tecnologías de lectores de tarjetas

- Investigar las distintas tecnologías expuestas anteriormente en profundidad. Cada grupo estudiará una.
- Extraer los datos más característicos y llamativos de las mismas.
- Observar y determinar los niveles de implantación de cada una de ellas.
- Clasificar las áreas de uso de cada una de ellas.
- Preparar una presentación con PowerPoint o con Prezzi, para exponer por grupos en clase, con los datos obtenidos en la investigación.
- Presentar también las conclusiones de los datos obtenidos y dos preguntas que os hayan resultado interesantes y deseéis realizar al resto de grupos, basándoos en algún elemento del estudio realizado.

Metodología:

- Cada grupo trabajará una de las tecnologías de manera que después la expondrá al resto de compañeros de la clase
- Los grupos se formarán dependiendo del alumnado por clase, preferiblemente de un máximo de tres alumnos, aunque dependerá del número en alumnos en el aula. Se podrán repetir tecnologías y que sean dos grupos los que trabajen una en concreto.
- La agrupación de los alumnos se puede realizar de manera espontánea, o bien bajo el criterio del docente.
- Sería oportuno que todos los alumnos participasen en la exposición, así conseguiremos que todos se esfuercen en perfeccionar su capacidad de oratoria y de explicación en grupo. Esta capacidad les será necesaria en su próxima vida laboral.

Elementos híbridos o mixtos

Al hablar de elementos híbridos o mixtos, la atención se centra en aquellos elementos que, en sí mismos, incorporan varias tecnologías y/o detectores de los citados en el Apartado 2.5.1.

Un ejemplo sería el que se expone en la Figura 2.31, donde se observa un lector de tarjetas RFID junto a un teclado numérico y que en algunos casos también incorpora la lectura de una característica biométrica, como por ejemplo la huella dactilar.

Figura 2.31. *Elemento híbrido de control de acceso. Lector NFC con teclado numérico.*

Este tipo de elementos aumentan el nivel de seguridad de manera exponencial, ya que superpone varias técnicas de reconocimiento en el acceso.

2.5.2. Teléfono intercomunicador. Monitor de hogar

El teléfono o el monitor serán los elementos que el usuario tendrá en su hogar para poder interactuar con el resto del sistema. El teléfono solo permitirá una comunicación en audio con la placa de calle, mientras que el monitor permitirá observar el exterior gracias a la cámara de la placa de calle.

Poseen una pequeña botonera que permite controlar el funcionamiento del sistema, además de dar la capacidad de abrir la puerta, encender una luz exterior (si así está preinstalado) y llamar a la persona responsable de la conserjería (en instalaciones comunitarias con este servicio).

En ambos casos, la comunicación con el resto de elementos, como se expuso en el Apartado 2.3, se realiza con cable plano multihilo.

Existen dos **tipos de teléfonos** o monitores:

- **Estándar:** la comunicación se realiza al descolgar el terminal de la vivienda, pudiendo escuchar cualquier conversación existente entre la placa de calle y cualquier otro teléfono.
- **Secreto:** la comunicación solo se realiza cuando se ha llamado al teléfono o monitor, solo se establece esa conexión, por tanto, no permite la escucha de conversaciones ajenas.

También permiten el control de volumen, ajuste de brillo y otros parámetros audiovisuales, además de la capacidad de apagar el dispositivo ubicado en el hogar para evitar molestias.

2.5.3. Alimentación y distribución

Los elementos de alimentación y distribución son el instrumental necesario para el correcto funcionamiento de los elementos de la instalación. El primero, al llevar la energía, es el que al final posibilita el funcionamiento general; el segundo, permitirá que la información llegue al usuario final.

- **Elementos de alimentación:** debido a que los elementos de la instalación no trabajan con el voltaje suministrado por la red eléctrica convencional, es necesaria la instalación de elementos de alimentación específicos para este tipo de instalaciones, estos vienen ya preparados con distintos voltajes de salida dependiendo de qué elementos de la instalación requieran de su alimentación, así:
  - — Los circuitos de audio necesitarán 12 V en corriente alterna (12 Vac).
  - — Los circuitos de vídeo necesitarán 18 V en corriente continua (18 Vcc).
  - — La alimentación al distribuidor necesitará 12 V en alterna y 12 V en continua a la misma vez para distintas partes de este.

  Dependiendo del tipo de instalación, será necesario el elemento que cubra todas las necesidades energéticas.
- **Elementos de distribución:** serán los encargados de redireccionar la imagen obtenida por la cámara de la placa de calle y llevarla hasta la pantalla de un monitor concreto. Similar a los elementos de distribución utilizados en las instalaciones de ICT.

2.5.4. Placa de calle y abrepuertas

Estos elementos son parte importante de la instalación ya que son los dispositivos que se encuentran expuestos al exterior y son los que controlan el acceso, objetivo que se quiere conseguir con estas instalaciones.

- **Placa de calle:** dispositivo exterior de la instalación en el cual se encuentra la botonera de llamada a los distintos hogares con los que cuenta la instalación. Las dimensiones del mismo dependerán del número de usuarios que existan en la comunidad o de un único pulsador si es en una vivienda unifamiliar.

  Mediante multiplexación, realiza la conexión con los distintos usuarios. Incluye cámara de vídeo para la captación de imágenes de amplio campo de visión y amplificadores de audio para la correcta comunicación.
- **Abrepuertas:** elemento de tipo electromagnético que permite la apertura de la puerta cuando se pulsa el botón de apertura en el monitor de hogar. Esta señal será generada por la placa de calle activando un electroimán ubicado en este elemento.

Vocabulario

Multiplexación: es la operación llevada a cabo mediante multiplexores, esto es, seleccionar la información recibida por una de sus entradas del multiplexor (o multiplexador) y ubicarla en la salida. Podría generalizarse como un conmutador por selección.

En la Figura 2.32 se observa un demultiplexor que realiza la función inversa al multiplexor. Toma el valor de la entrada y la coloca en la salida seleccionada.

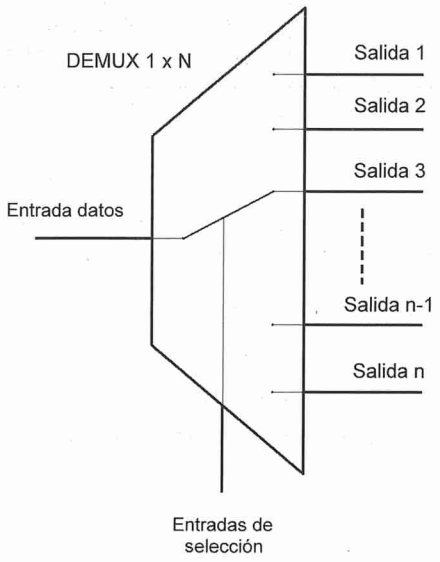


Figura 2.32. *Esquema general de un demultiplexor de una entrada y N salidas.*

2.5.5. Instalaciones de videoportero IP

Se trata de un módulo que, conectado a la placa de calle, permite una conexión inalámbrica entre la instalación de videoportero y los monitores de hogar, que ahora podrán ser sustituidos por elementos específicos para esta funcionalidad o incluso dispositivos móviles que se conectan y configuran a través de aplicaciones específicas según el fabricante.

También permite la comunicación de manera cableada sin realizar más instalación de cable, ya que utiliza la estructura de xDSL del cableado de internet existente.

Recuerda:

Las siglas xDSL se refieren de manera genérica a las tecnologías de comunicación ADSL o VDSL, según corresponda.

2.6. Circuitos cerrados de televisión

Los circuitos cerrados de televisión (CCTV) son instalaciones de seguridad que utilizan cámaras de captación continua de imágenes sobre la zona que se quiere proteger. Hablamos de captación de imágenes, ya que la grabación de las mismas no la realizan las cámaras, sino el resto de elementos de los que se compone la instalación y de los cuales se tratará a lo largo de este apartado.

Los CCTV, de todas formas, deben asegurar, en caso de acto delictivo, poder responder a las siguientes tres preguntas:

- ¿Qué acto delictivo se está cometiendo?
- ¿Quién está cometiendo el acto delictivo?
- ¿Dónde se está cometiendo el acto delictivo?

Los CCTV realizan un tipo de seguridad llamada de **protección pasiva.** Se denomina protección pasiva debido a que no evita ni soluciona el problema de un robo, incendio, etc., simplemente da la posibilidad avisar, en algunos casos, cuando alguno de los hechos delictivos se están realizando o a la hora de recabar pruebas visuales del delito cometido.

Aunque se ha hablado de ello en estas líneas, los elementos principales que compondrán una instalación de CCTV serán: las cámaras, los videograbadores (DVR, *Digital Video Recorder*) y los dispositivos de almacenamiento.

Recuerda:

Para que una instalación de CCTV sea considerada correcta, debe responder de manera inequívoca a las tres preguntas: ¿qué?, ¿quién? y ¿dónde? sobre el acto delictivo que se quiere probar.

A nivel legal, se mantiene la normativa relativa a seguridad expuesta en el Apartado 2.2 de esta unidad, con especial atención al Apartado 2.2.2, donde se estudió la parte de la normativa referente a la **protección de los datos** de los usuarios, según la nueva LGPD, además de cómo deben ser tratados y almacenados.

2.6.1. Cámaras. Elementos de captación

Las cámaras, sin lugar a dudas, serán el elemento primordial de este tipo de instalaciones; es por esto que, su elección será muy importante para que la instalación sea lo más correcta y de la mayor calidad posible.

Se puede definir la **función principal de una cámara** como la captura de la luz reflejada en los objetos que se encuentran en su CdV (campo de visión) para convertirla en una señal analógica o digital, típicamente conocida como señal de vídeo, capaz de ser trasmitida de manera cableada o inalámbrica al dispositivo de grabación y muestreo. También, si tiene esta capacidad, ocurrirá lo mismo con el audio del lugar.

Clasificación de las cámaras

Podemos diferenciar estas cámaras de manera general atendiendo a los siguientes parámetros:

- **Interior o exterior:** se debe diferenciar entre las usadas en instalaciones interiores y exteriores, no porque su funcionalidad varíe en gran medida, sino porque sus características físicas y carcasas están preparadas para sufrir la intemperie en el caso de las exteriores, mientras que la interiores no.
- **Cableadas o inalámbricas:** este es el método de comunicación que utilizarán para conectarse al dispositivo DVR.
- **Color, blanco y negro o infrarroja:** es la cantidad de longitudes de onda de la luz que será capaz de percibir.

Figura 2.33. *Distintos tipos de cámaras utilizados en sistemas de CCTV.*

En la Tabla 2.2 se muestra la clasificación.

Según su **forma,** las cámaras pueden recibir otra clasificación, las principales existentes en la actualidad son:

- Cámaras **cube,** para interior.
- Cámaras **box,** para interior.
- Cámaras **bullet,** para exterior.
- Cámaras **domo,** para interior y exterior.

Tabla 2.2. Clasificación general de las cámaras usadas en CCTV

Tipo de cámara	Características
Cámaras de interior	Son las mejores en cuanto a calidad y precio, además de ser las más sencillas de instalar al no necesitar mecanismos ni protecciones especiales.
Cámaras de exterior	Están preparadas para resistir las inclemencias climáticas, ya que se utilizan en espacios abiertos principalmente. Incorporan carcasas y protecciones en las conexiones para prevenir cualquier fallo de funcionamiento.
Cámaras antivandálicas	Son un tipo de cámaras de exterior, preparadas para evitar su rotura ante posibles actos vandálicos, robos o manipulaciones. Suelen colocarse en lugares de pública concurrencia.
Cámaras con movimiento y zoom	Son cámaras motorizadas que dan la posibilidad al usuario o a la central de seguridad de moverlas sobre su estructura para visualizar el entorno donde se encuentran.
Cámaras ocultas o espía	Son pequeñas cámaras que están escondidas dentro de otros objetos con el fin de pasar desapercibidas.
Cámaras de infrarrojos	También denominadas de visión nocturna, se basan en capturar el espectro de luz que genera la energía infrarroja creando una imagen en blanco y negro. Suelen incorporarse en cámaras diurnas, que, a través de un detector de luz incluido en la cámara, cambia el funcionamiento en el momento en que se carece de luz.
Cámaras IP (*Internet Protocol*)	Están preparadas para trabajar de manera cableada o inalámbrica, mediante wifi, y ser conectadas directamente a internet, permitiendo desde la distancia visualizar las imágenes en tiempo real con las aplicaciones oportunas.
Cámaras todo en uno	Este tipo de cámaras las componen aquellas que tienen una instalación mucho más libre que las anteriores, partiendo de la posibilidad de ponerlas en el interior o el exterior y que no necesitan cableado, ya que poseen conexión por wifi (habría que hacerles llegar la alimentación eléctrica).

Características de las cámaras

A la hora de seleccionar los dispositivos de captación de imágenes, deberemos tener en cuenta qué servicios pueden ser obtenidos de ellos, no todos valen para todo, por eso deberemos tener en cuenta los siguientes aspectos técnicos:

- **Resolución:** la resolución es la cantidad de puntos de los que se puede obtener información. A cada punto, en los sistemas digitales, se le denomina píxel; por ejemplo, una cámara que sea capaz de percibir 1360 × 768 píxeles, distinguirá entre 1360 píxeles en la horizontalidad y 768 en la verticalidad.

  Si sobre los datos anteriores se operan las cantidades, obtenemos 1360 × 768 = 1 044 480 píxeles, lo que llevaría a decir que la cámara tiene una resolución de 1 megapíxel (1 MP).

  Con una resolución mayor, se conseguirá obtener mucha más información en cada fotograma tomado.

- **Cobertura o campo de visión (CdV):** se trata del área que la cámara es capaz de cubrir con la lente que posee, medida en grados. En este punto, habrá que destacar las siguientes cámaras:
  - — *Cámaras direccionales:* son aquellas que capturan las imágenes en una sola dirección.
  - — *Cámaras motorizadas:* se trata de cámaras direccionales que incluyen un motor en su sujeción que permite mover el campo de visión a decisión del usuario.
  - — *Cámaras 360º:* composición de varias lentes con campos de visión solapados, de manera que dan capacidad a la cámara para capturar una imagen completa del entorno que le rodea.

Vocabulario

Luz policromática: haz único de luz que contiene la información de varios colores.

Haz monocromático: haz de luz de un solo color y, por tanto, una única longitud de onda.

Espejos dicroicos: espejos colocados en forma de prisma capaces de dividir un haz de luz policromática en diversos haces monocromáticos.

CCD (*Charge-Coupled Device*): sensor con diminutas células fotoeléctricas que registran la imagen.

- **Lentes:** son las encargadas de que la imagen capturada no tenga ningún tipo de distorsión, y de ellas dependerá: la cantidad de luz que se capture y el tamaño de la escena de la que se quiere tomar la imagen. La correcta elección de la lente, debe asegurar que:
  - — La luz que acceda al CCD sea la correcta para que la trasmisión de la luz sea eficiente.
  - — Tenga una gran resolución y contraste.
  - — La imagen que se captura sea fiel a la realidad.

Recuerda:

La escala en la Tabla 2.3 resalta la relación existente entre la horizontalidad y la verticalidad. A modo de ejemplo, la escala 16:9 está resaltando que existen 16 píxeles horizontales por cada 9 verticales.

Tabla 2.3. Formatos de resolución en cámaras de CCTV

Resoluciones											
Estándar	CIF	2CIF	4CIF	D1	VGA	HDTV (720 p)	1.3 MP	2 MP	Full HDTV (1080 p)	3.1 MP	5 MP
Resolución horizontal (en píxeles)	352	704	704	720	640	1280	1280	1600	1920	2048	2592
Resolución vertical (en píxeles)	240	240	480	480	480	720	1024	1200	1080	1536	1944
Escala	22:15	44:15	22:15	3:2	4:3	16:9	5:4	4:3	16:9	4:3	4:3
Tipo de cámara (A: analógica; D: digital)	A	A	A	A	D	D	D	D	D	D	D

Actividad resuelta 2.1

Colocación de cámaras en una instalación

(La actividad, los planos y elementos que aparecen como imágenes se han obtenido usando la aplicación IP Video Design Tool de la empresa JVSG, cuyo enlace se puede encontrar al final de la unidad. Las personas que aparecen en las siguientes imágenes son utilizadas por el programa de manera automática para observar las distancias correctas del campo de visión.)

Teniendo en cuenta las características especificadas sobre cámaras de seguridad, se debe distribuir en el siguiente plano las cámaras de seguridad necesarias para una correcta instalación de seguridad.

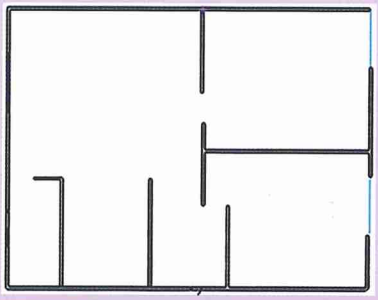


Figura 2.34. *Plano del local donde irá la instalación.*

Solución:

En primer lugar, habrá que localizar cuáles son los puntos de acceso con los que cuenta esta vivienda en concreto. En la Figura 2.35 se observa la existencia de cuatro ventanas y una puerta.

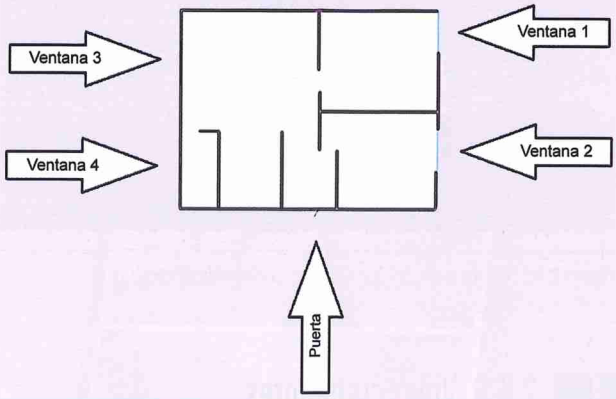


Figura 2.35. *Vías de acceso al local.*

Tras encontrar las vías de acceso, se debe (dependiendo del nivel de instalación del hogar digital a instalar) observar dónde colocar las cámaras de manera que todas ellas queden cubiertas. Como podemos ver, la ventana cuatro da acceso al baño, luego este es el único sitio donde no podrá haber cámara instalada.

Antes de ubicar las cámaras, habrá que discernir las características de estas y se tendrá en cuenta: zoom, altura de instalación, distancia focal, alto, ancho y profundidad del campo de visión y resolución. Todo ello para que el área y las imágenes sean lo más nítidas posible.

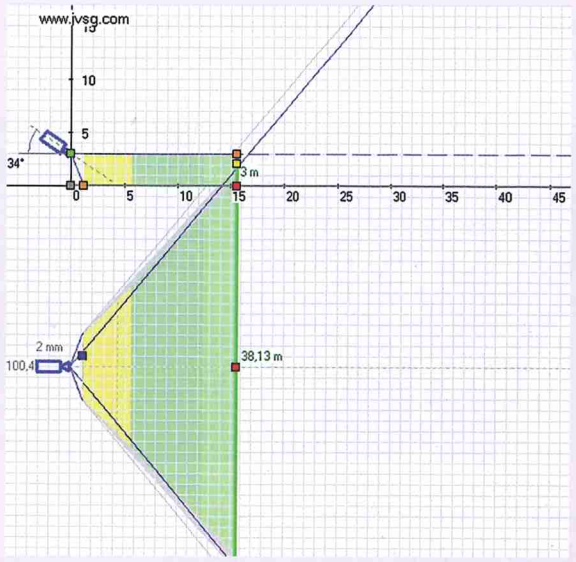


Figura 2.36. *Ángulos de visión de la cámara.*

Se puede observar cómo esta cámara (Figura 2.36), colocada a 3 metros de altura, percibe la imagen a partir del metro 2 y a partir del 5 comienza a ser una imagen de calidad aceptable. Los niveles de calidad se observan en el color del campo de visión: amarillo calidad media, verde oscuro calidad media alta, verde claro calidad alta. Todo aquello que no esté en la zona coloreada se percibirá si está en el campo de visión de la cámara, pero no se asegura la correcta calidad de las imágenes obtenidas.

Colocando esta cámara en el plano descrito, se podrá controlar un plano bastante amplio (Figura 2.37).

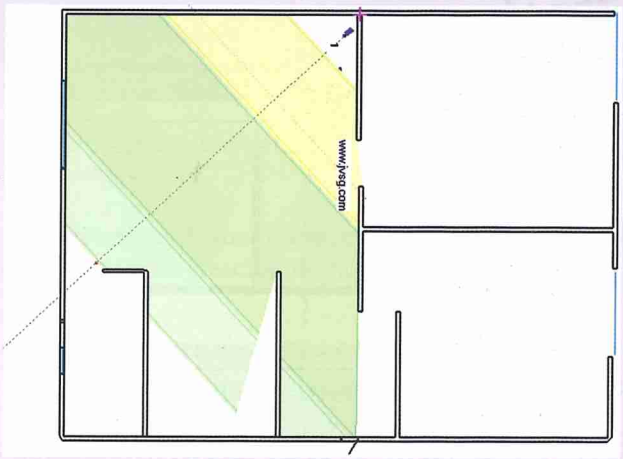


Figura 2.37. *Plano con el área captada por la cámara 1.*

Al colocar la cámara 1 en el lugar que se observa, todo el hueco amplio del salón queda visualizado de una manera correcta, además se capta la posible intrusión a través de la ventana del aseo, evitando instalar una cámara en este espacio.

La imagen que obtendríamos de esta cámara es la mostrada en la Figura 2.38.

Figura 2.38. *Imagen de la cámara 1.*

Del mismo modo, iremos colocando cámaras hasta completar todo el espacio a proteger de la vivienda, en este caso se han utilizado cuatro cámaras: la del salón, una en cada dormitorio y otra controlando el acceso a través de la puerta.

El plano quedaría como el mostrado en la Figura 2.39.

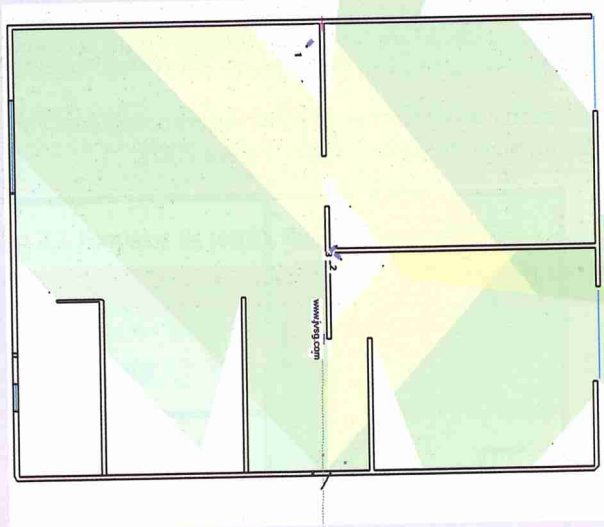


Figura 2.39. *Plano con el área protegida al instalar todas las cámaras.*

En las Figuras 2.40 a 2.42, se muestran las imágenes obtenidas de cada una de las cámaras instaladas.

Figura 2.40. *Imagen de la cámara 2 en el dormitorio 1.*

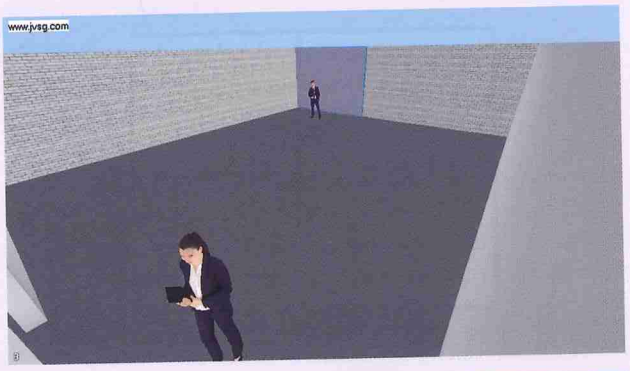


Figura 2.41. *Imagen de la cámara 3 en el dormitorio 2.*

Figura 2.42. *Imagen de la cámara 4 en la entrada al recinto.*

2.6.2. Videograbadores

Al hablar de los videograbadores, la atención se centra en los elementos que se encargan de recibir las imágenes capturadas por las cámaras de la instalación y prepararlas para ser visualizadas a través de los monitores o almacenadas en los elementos de almacenamiento.

Algunos videograbadores, utilizados sobre todo en el siglo XX, y de los cuales aún quedan en algunas instalacio-

nes privadas, realizan el almacenamiento en dispositivos y elementos analógicos, como es el caso de las cintas de VHS.

En la actualidad, la inmensa mayoría de los dispositivos DVR (*Digital Video Recorder*) trabajan ya con tecnología digital de almacenamiento, es decir, utilizan las unidades binarias para la codificación y el almacenamiento de la información. También se pueden centralizar en PC destinados a esta función gracias a las tarjetas gráficas diseñadas para esta función y a las aplicaciones y el software diseñados para gestionar esta información.

Para la codificación de las imágenes, los DVR realizan las siguientes funciones:

- **Función MUX:** utiliza la **demultiplexión o demultiplexación** (función inversa a la multiplexación explicada anteriormente), de modo que puede seleccionar la información suministrada por una de las cámaras en concreto y posicionarla en el monitor y en el elemento de visionado.
- **Función SEC:** utiliza la **secuenciación** para el visionado y almacenamiento de la información de las cámaras. Dicho de otro modo, crea una secuencia automática ordenada para visionar la información de las cámaras, una detrás de otra, pero viendo una sola en cada instante de tiempo. Normalmente, el tiempo de visionado es un parámetro que se puede modificar, además se puede fijar una de las imágenes de manera manual.
- **Función QUAD:** utiliza la **cuadriculación** para el visionado y almacenamiento, es decir, divide la pantalla en una cuadrícula de N×N celdas, y muestra a la misma vez la información de todas las cámaras conectadas, cada una en una de las celdas que se divide la nueva imagen.

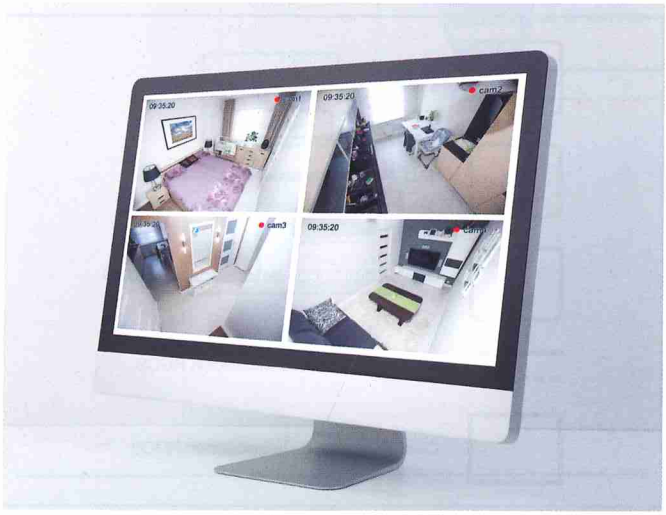


Figura 2.43. *Imagen resultante de un DVR con función QUAD 2x2.*

2.6.3. Elementos de visionado y almacenamiento

Aunque son funcionamientos diferentes, se agrupan estos dispositivos en el mismo apartado al tratarse de elementos terminales o finales de las instalaciones, donde se recabarán las pruebas necesarias y llegado el caso revisar un acto vandálico en el lugar protegido.

Monitores

Son dispositivos capaces de tomar una señal eléctrica con una codificación específica (analógica o digital) y convertirla en una imagen visible para el ojo humano.

El abanico de dispositivos de visionado es tan amplio que dependerá de la calidad que queramos obtener, la información que se va a mostrar, etc., así que su elección dependerá de las necesidades del usuario.

Dependiendo del tipo de servicio contratado, el monitor se encontrará instalado a nivel local en la vivienda, en el cuarto de seguridad, o a nivel remoto en las instalaciones del CRA. También, y dependiendo de la tecnología usada, existirá la posibilidad de recibir las imágenes generadas por el DVR en algún dispositivo móvil (*smartphone* o tableta) del usuario.

Figura 2.44. *Centro de control de CCTV de la empresa de seguridad. Local o remoto.*

Algunos **tipos de monitores,** en función de la tecnología empleada para la creación de las imágenes por parte del DVR, son:

- Monitor con tubo de rayos catódicos o CRT (*Cathode Ray Tube*). Tecnología analógica o digital. Comunicación por cable coaxial o VGA.
- Pantalla de cristal líquido o LDC (*Liquid Crystal Display*). Tecnología analógica o digital. Comunicación por cable coaxial, VGA o euroconector.

- Pantalla de plasma o PDP (*Plasma Display Panel*). Tecnología analógica o digital. Comunicación por cable coaxial, VGA o euroconector.
- Transistor de películas finas o TFT (*Thin Film Transistor*). Tecnología digital primordialmente. Comunicación por VGA, euroconector, USB o HDMI.
- Pantallas de diodos emisores de luz o LED (*Light Emitting Diode*). Tecnología digital. Comunicación por VGA, euroconector, USB o HDMI.

Las **características principales** a tener en cuenta a la hora de elegir un monitor son:

- Resolución: cantidad de píxeles que puede mostrar en el área visible de la pantalla.
- Tamaño: medido normalmente en pulgadas, es la medición de la línea diagonal que atraviesa la pantalla.
- Método de generación de la imagen (ya expuestos anteriormente).
- Definición: se entiende como la capacidad del dispositivo de mostrar imágenes lo más reales posible, se basa sobre todo en la resolución que posee. Podemos clasificarla en baja definición (LD), media definición (MD), alta definición (HD) o ultra alta definición (ultra HD). Esta última se puede considerar en la actualidad como ver la imagen como se vería en la realidad.

Dispositivos de almacenamiento

Los dispositivos de almacenamiento son los elementos para almacenar de manera física la información obtenida de las cámaras. Deben estar a disposición ante cualquier solicitud de las Fuerzas y Cuerpos de Seguridad del Estado en cualquier situación de violación de la seguridad. Estos son:

- **Cintas magnéticas:** es una técnica de tecnología analógica ya en desuso, la información se almacena de manera secuencial en una cinta magnética.
- **Memorias USB:** el dispositivo de almacenamiento se encuentra conectado al elemento DVR para realizar una copia local de las imágenes obtenidas.
- **Discos duros:** son elementos digitales de gran capacidad de almacenamiento que se podrán utilizar de manera local o remota.
- **PC:** son los dispositivos informáticos de gestión y control del sistema CCTV, pueden ser también los encargados del almacenamiento de la información suministrada por las cámaras.
- **Almacenamiento en la nube (*cloud*):** los datos se almacenan en un espacio que la empresa que presta el servicio tiene adquirido en servidores secundarios accesibles desde internet. Supone un abaratamiento de costes, ya que este espacio va incluido en el precio del servicio y no requiere dispositivos específicos.

Los medios de comunicación entre ellos serán los necesarios y estarán acorde a la cantidad de información suministrada para no ralentizar la lectura y la escritura de la misma.

2.7. Canalizaciones y locales

Las canalizaciones en la vivienda donde se realice la instalación, si es obra nueva, deberán ser expresas para la instalación de seguridad, intentando evitar la proximidad con las líneas eléctricas para que no haya interferencias en las señales transmitidas.

En viviendas ya construidas, se podrán utilizar las canalizaciones existentes de la instalación de ICT existente, como anteriormente intentando evitar la proximidad a líneas de transmisión eléctrica.

Todos los elementos, a través de las centrales de alarma y las canalizaciones de seguridad, estarán conectados a la pasarela para su comunicación exterior (Ley sobre seguridad privada INT/314/2011, de 1 de febrero).

Las canalizaciones de seguridad, según la Guía técnica de aplicación del Ministerio de Industria, Comercio y Turismo ITC-BT-51 Guía E Feb 07 en la que quedan reguladas la distribución e instalación, se consideran parte de las canalizaciones de la instalación domótica.

En las siguientes imágenes (Figuras 2.45 a 2.53), como aclaración, se muestran las adaptaciones de la guía técnica para las canalizaciones de seguridad para el desarrollo de la red RGCS en el hogar digital.

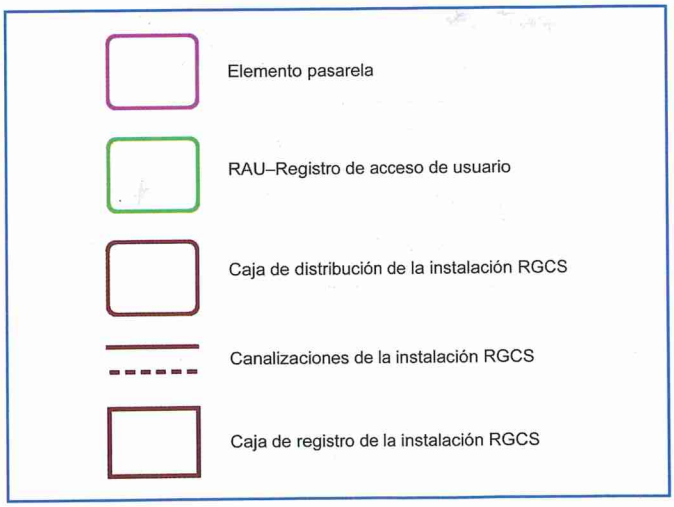


Figura 2.45. *Leyenda de las canalizaciones de una instalación en la red RGCS.*

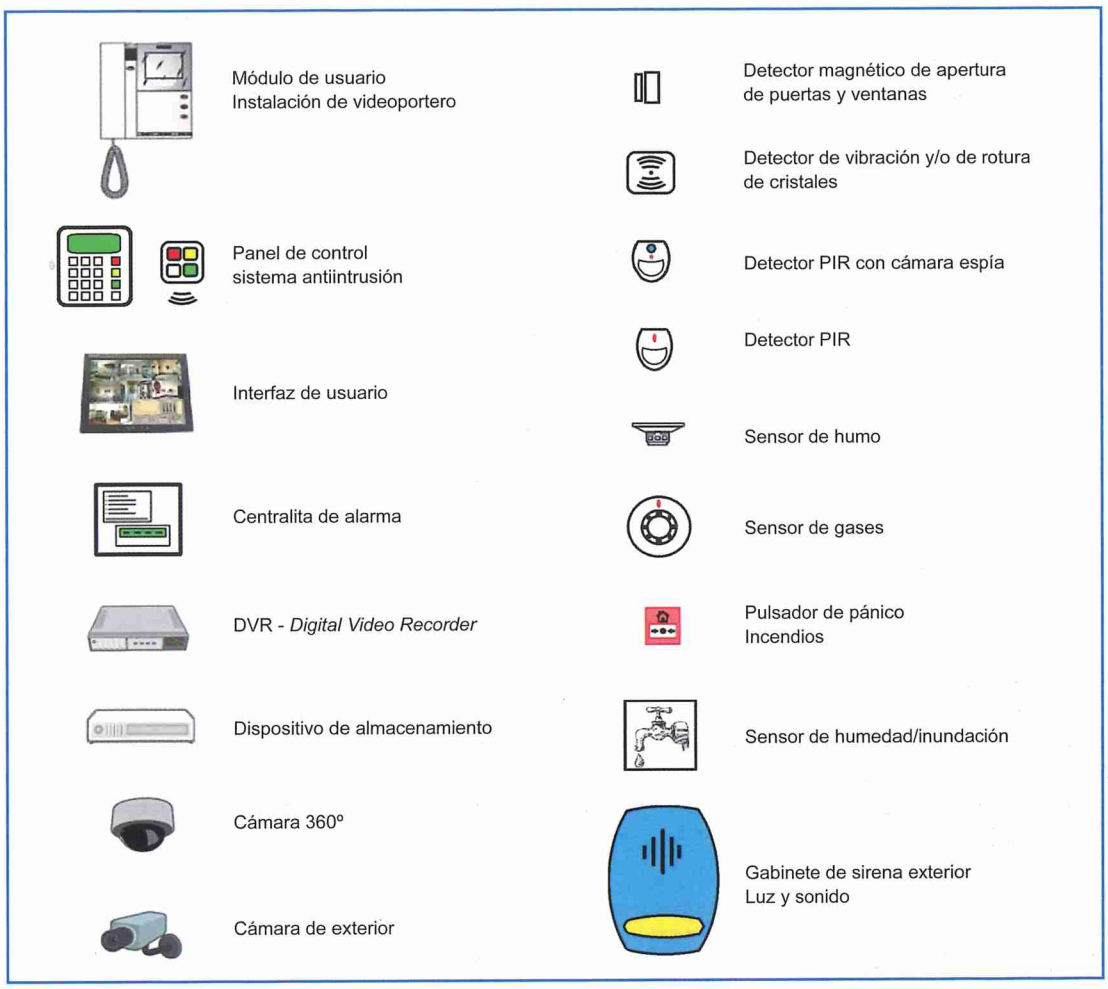
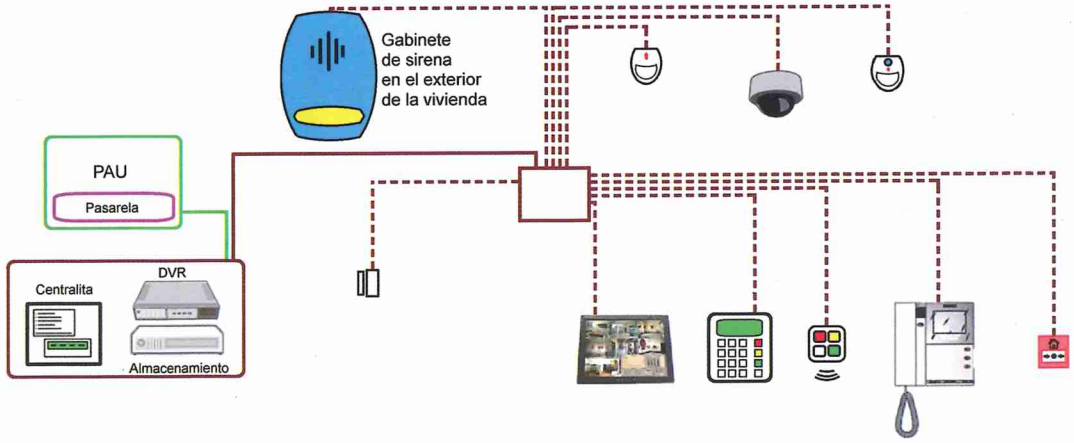
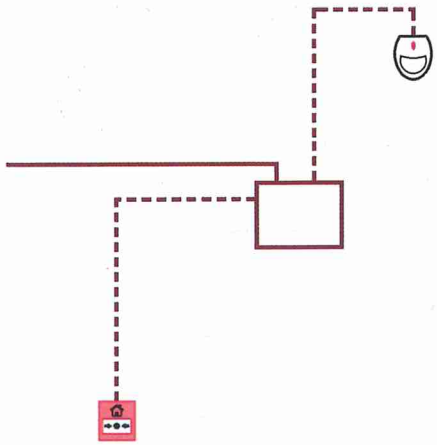


Figura 2.46. *Leyenda de los elementos generales de una instalación en la red RGCS.*



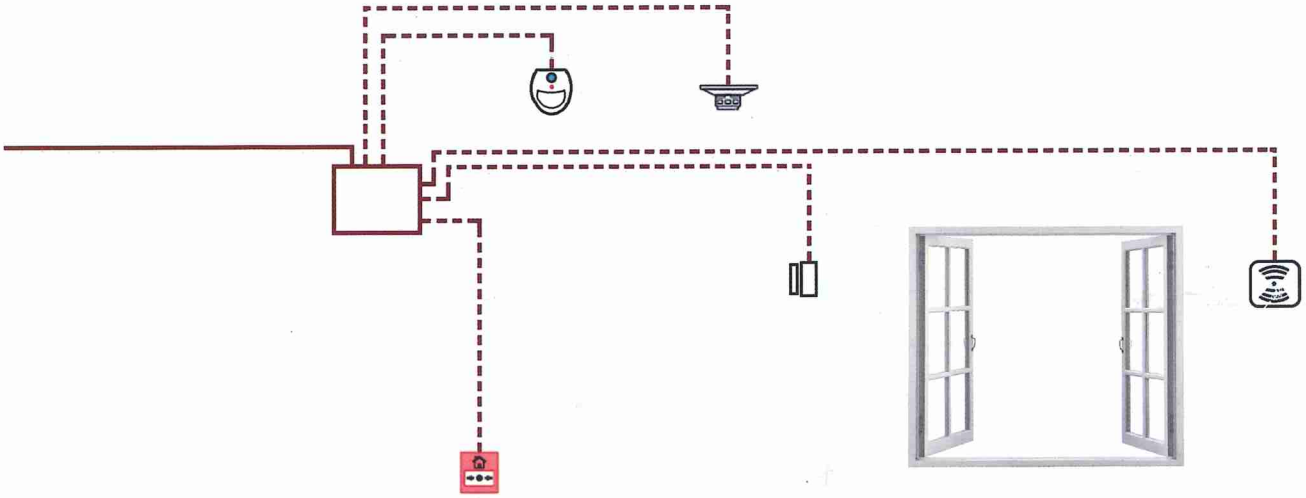
Línea de suelo

Figura 2.47. *Canalizaciones en el vestíbulo de la vivienda.*



Línea de suelo

Figura 2.48. *Canalizaciones en el pasillo de la vivienda.*



Línea de suelo

Figura 2.49. *Canalizaciones en el salón comedor de la vivienda.*

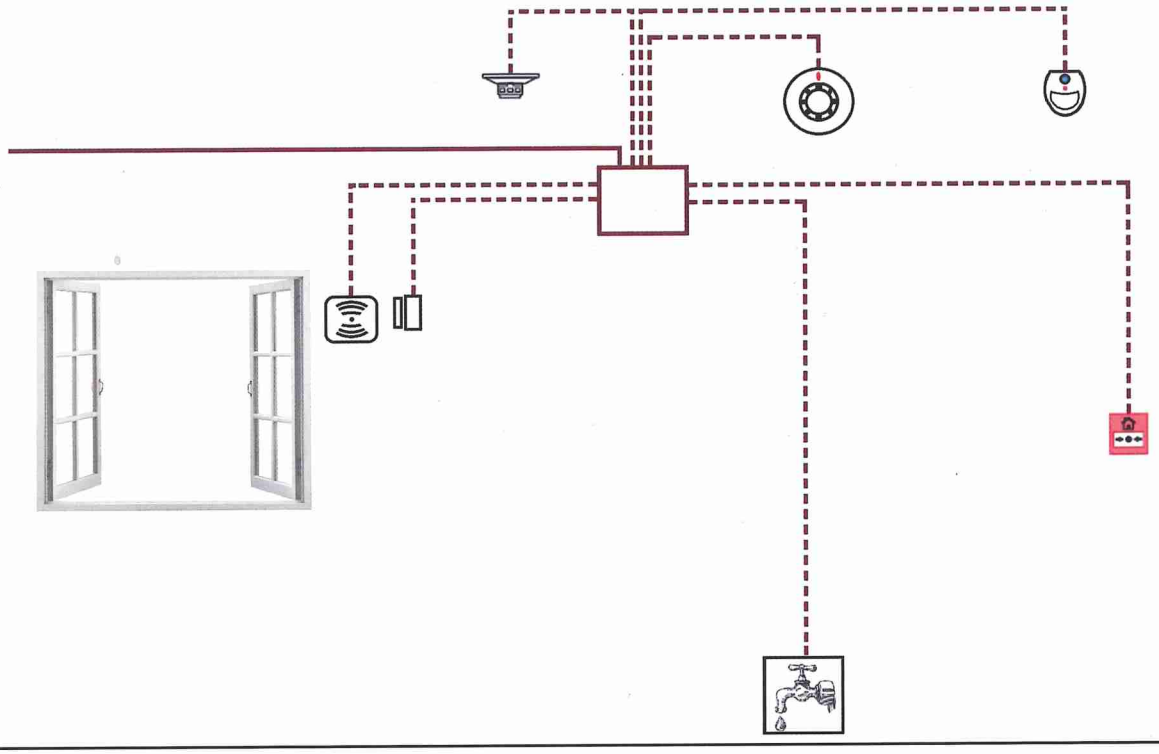


Figura 2.50. *Canalizaciones en la cocina de la vivienda.*

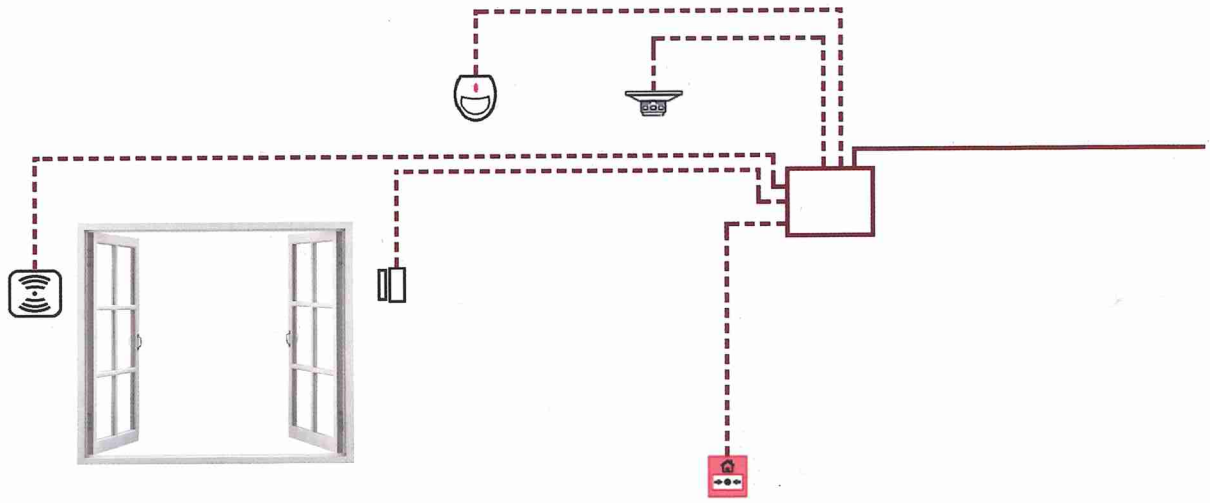


Figura 2.51. *Canalizaciones en los dormitorios de la vivienda.*

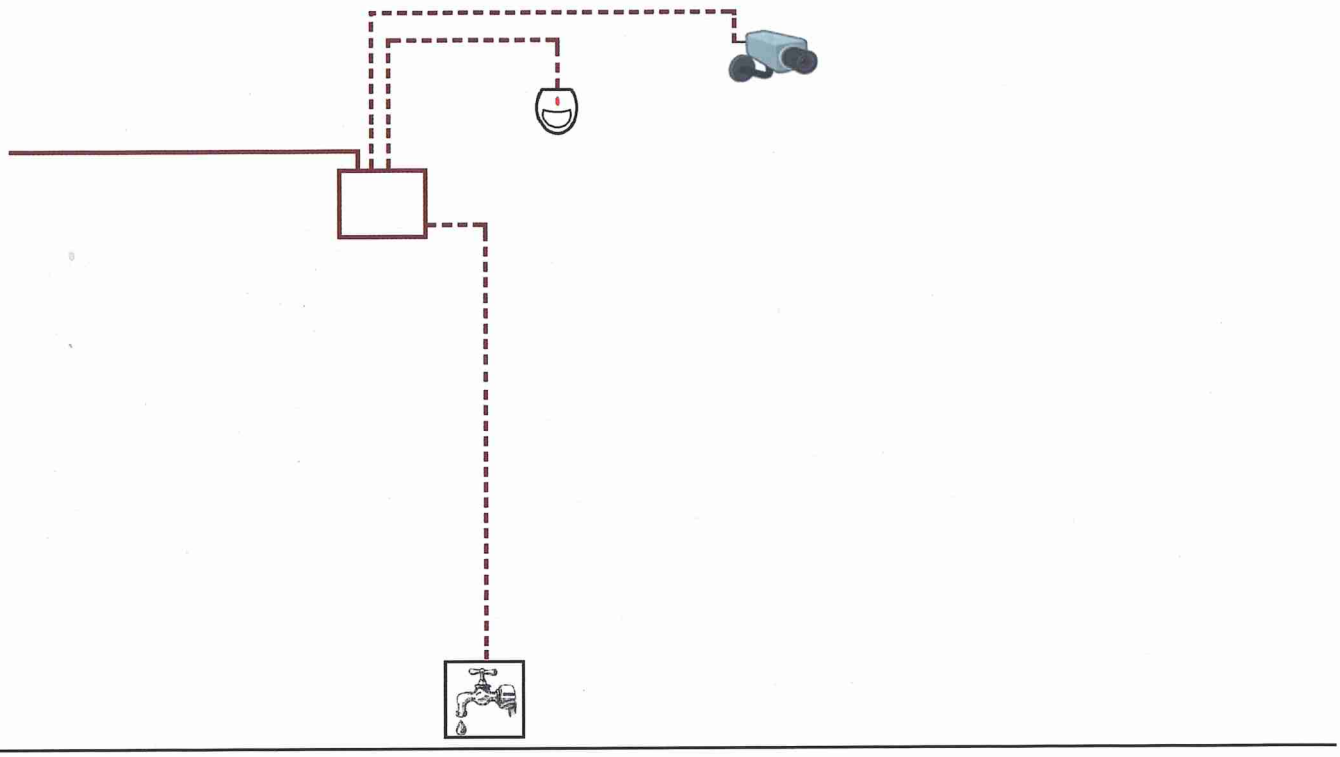


Figura 2.52. *Canalizaciones en la terraza o el patio de la vivienda.*

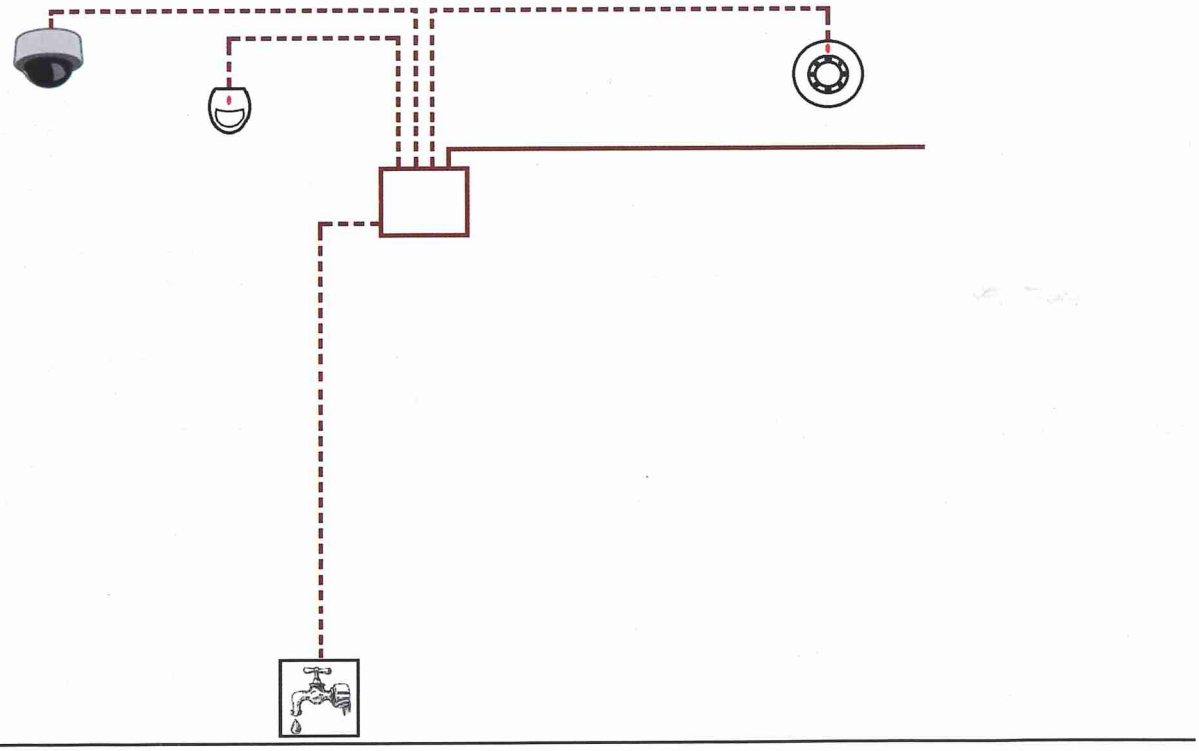


Figura 2.53. *Canalizaciones en la cochera o garaje de la vivienda.*

Las canalizaciones y distribuciones expuestas hasta el momento se ciñen al interior de la vivienda y atendiendo a que se realicen sobre una vivienda unifamiliar. Cuando esta implantación de la seguridad se realiza en **una instalación comunitaria,** puede que ciertos servicios de esta área recaigan sobre un **centro de control común.**

En este caso, se deberá atender a lo que expone la ley sobre seguridad privada. A continuación, se muestra un extracto de la Ley sobre Seguridad Privada, Orden INT/316/2011, de 1 de febrero, creado a tal efecto.

«Los sistemas para la recepción y verificación de las señales de alarmas estarán instalados en un centro de control, cuyo local ha de reunir las siguientes características:

a) Carecer de paredes medianeras con edificios o locales ajenos a los de la propia comunidad.
b) Acristalamiento de blindaje antibalas.
c) Doble puerta blindada de acceso con sistema conmutado tipo esclusa y dispositivo de apertura a distancia, debiendo ser este manual desde su interior.
d) Las paredes que delimiten o completen la zona no acristalada de la sala de control con alto grado de resistencia.
e) Control de los equipos y sistemas de captación y registro de imágenes.
f) Sistema de interfonía en el control de accesos.
g) La sala de control siempre estará atendida por dos operadores por turno, como mínimo.
h) Generador o acumulador de energía, con autonomía de veinticuatro horas, como mínimo, en caso de corte del fluido eléctrico.
i) Dispositivo de alarma por omisión (APO) que produzca la transmisión de una alarma a otra central autorizada en caso de desatención por los operadores en un plazo superior a diez minutos, para su comunicación inmediata a las Fuerzas y Cuerpos de Seguridad del Estado.
j) Contará con dos vías de comunicación, como mínimo, para la recepción y transmisión de las señales de alarma recibidas.»

2.8. Seguridad informática

Fuera de las instalaciones y los elementos que componen la red de seguridad de la RGCS del hogar digital, ha de tenerse en cuenta que toda la instalación estará conectada a internet, lo que conlleva la posibilidad de espionaje, ataques y modificaciones a la configuración de la instalación por parte de personas con conocimientos informáticos, como pueden ser *hackers* y *crackers*.

Es necesario por tanto que la pasarela de acceso a la instalación del hogar digital cuente con unas medidas de seguridad informática para evitar cualquiera de las situaciones citadas anteriormente.

Sabías que

Tanto un *hacker* como un *cracker* son personas que, a través de internet y sin permiso explícito, acceden a la red HAN y a los dispositivos conectados a la misma con distintos fines, pero con el mismo cariz ilegal.

Un *hacker* es una persona con amplios conocimientos que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos a través de internet con el fin de investigar y crear mejoras, sin que estas sean dañinas para el usuario del equipo informático.

Un *cracker* también es una persona de amplios conocimientos informáticos que accede ilegalmente a sistemas informáticos ajenos y a manipularlos con el fin, a diferencia de los *hackers,* de destruir e infectar el sistema informático afectado. En muchos casos son los creadores de la mayoría de los virus informáticos existentes y llegan a vender la información obtenida de los equipos invadidos.

La seguridad que debe incorporar nuestro sistema debe incluir:

- En primer lugar, evitar claves demasiado sencillas o que se puedan obtener de nuestros datos personales.
- **Cortafuegos (*firewall*):** software específico para bloquear a todos aquellos usuarios y aplicaciones que no cuenten con acceso autorizado en la red HAN.

  Al estar conectado a internet, nuestra pasarela debe poseer una arquitectura compatible con los sistemas y modelos extendidos en internet, estos son el modelo OSI y el modelo TCP/IP, en ambos casos, existe una coincidencia en los niveles más bajos de codificación de los protocolos, es ahí donde la pasarela ofrece mecanismos de seguridad para aplicaciones específicas, tales como servidores FTP y Telnet y que aplican mecanismos de seguridad cuando una conexión TCP o UDP es establecida.
- La pasarela debe tener la capacidad de crear una **VPN** (*Virtual Private Network*) en nuestro hogar y por tanto una conexión del mismo tipo para la comunicación con el exterior, de este modo nos ofrece:
  - **Autenticación:** cualquier equipo que desee conectarse a la red local (HAN) debe estar dado de alta como usuario aceptado. Para ello debe contar con un nombre de usuario y una contraseña válida en esta red.
  - **Creación de un túnel virtual:** la comunicación se realiza a través de un «túnel» creado en internet de manera que solo conecta ambos extremos de la comunicación. Garantiza una comunicación **privada y segura.** Varias fuentes hablan de una efectividad superior al 98 %.

— **Encriptación de la información:** la información se transmite codificada mediante claves que solo conocen las máquinas que han creado el túnel virtual del que se hablaba anteriormente.

2.9. Uso de Arduino para la creación de prototipos básicos de seguridad

Arduino es una placa microcontroladora programable de software libre, que permitirá crear prototipos de sistemas de seguridad básicos, sobre todo a nivel educativo, de ahí que este apartado muestre varios ejemplos de pequeñas instalaciones de seguridad creadas con este soporte. La programación y configuración de las placas Arduino se detallan en el Apéndice B del presente libro.

Todos los prototipos que aquí aparecen están diseñados en la plataforma online Tinkercad (su enlace se puede ver en la relación de páginas web al final de la unidad), que ofrece la posibilidad de tener de manera online y gratuita un laboratorio electrónico de pruebas con los elementos básicos para familiarizarse con este elemento. Existe una extensión de esta aplicación online de pago que ofrece más funcionalidades.

En cada actividad resuelta, se muestra un enlace suministrado por el autor para acceder a los montajes en la plataforma web expuesta en el párrafo anterior.

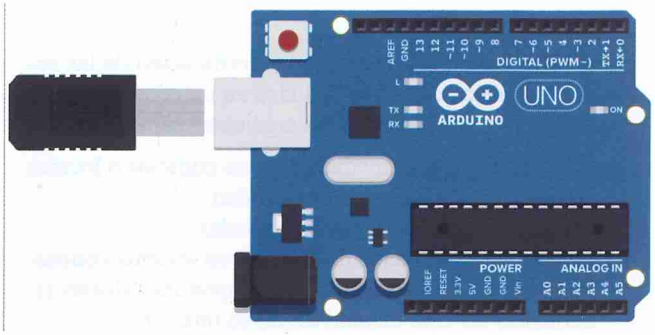


Figura 2.54. *Placa básica de Arduino UNO.*

Actividad resuelta 2.2

Control de acceso mediante sensor de presencia

El sistema controlado por Arduino generará cinco pitidos cuando el detector de presencia instalado frente a la puerta de acceso a la vivienda se active.

Los **elementos necesarios** para llevar a cabo la actividad son los que se pueden observar en la Figura 2.55.

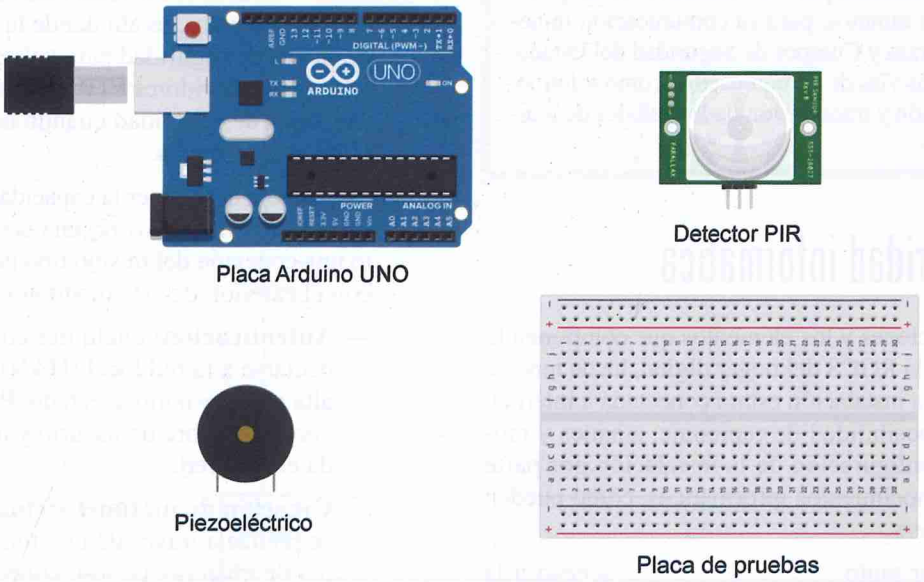


Figura 2.55. *Elementos necesarios para el montaje del circuito ejemplo.*

El **funcionamiento básico** del detector (PIR) y del actuador (piezoeléctrico) es el siguiente:

- **Detector PIR.** El detector cuenta con tres terminales de conexión. Los terminales de «Potencia» y «Tierra» irán conectados a los terminales del voltaje de alimentación. El terminal de «Señal» será el que envíe un valor de voltaje cuando un objeto se mueva dentro de su zona de detección. Si el objeto está dentro de la zona, el detector tomará un color rojo, a la vez que envía un voltaje distinto de 0 por el terminal de «Señal».

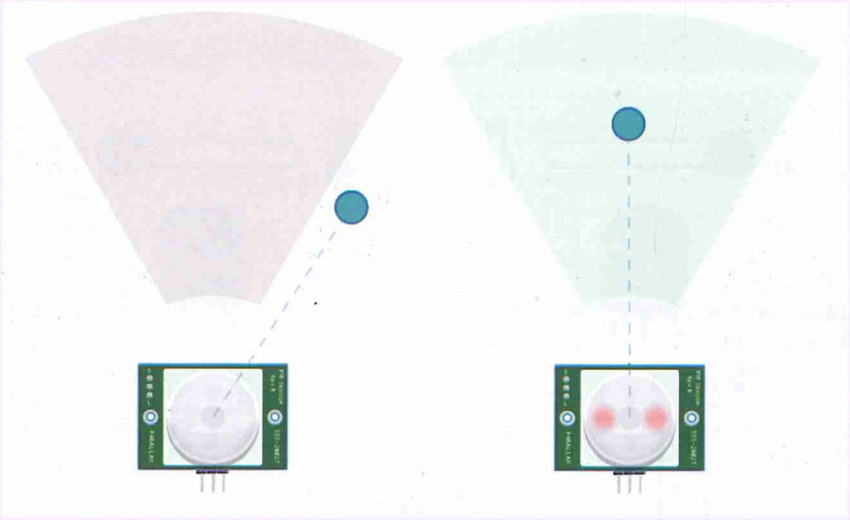


Figura 2.56. *Respuesta del detector PIR ante la presencia de un objeto en su campo de detección. Se observa a la izquierda el objeto fuera del campo de detección, a la derecha el objeto dentro de la zona.*

- **Piezoeléctrico.** Este dispositivo generará un pitido cuando llegue tensión a dos terminales, «Negativo» y «Positivo» respectivamente.

El **montaje** sería el mostrado en la Figura 2.57.

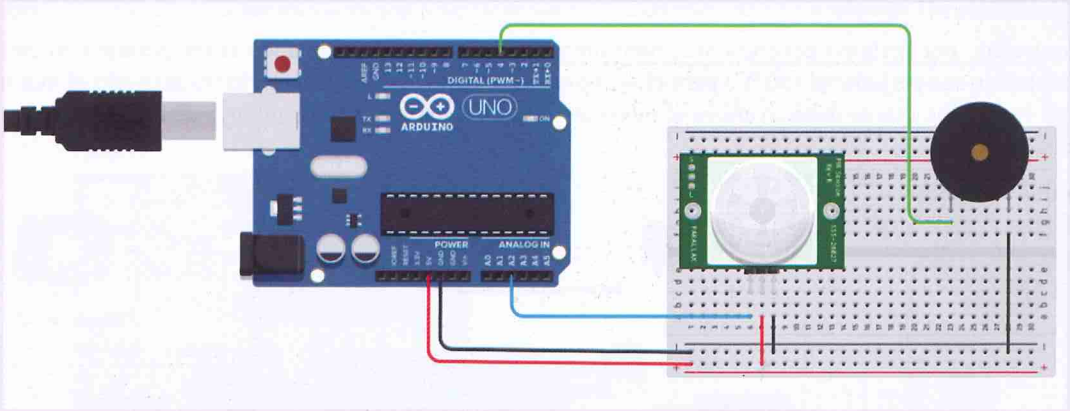


Figura 2.57. *Montaje completo del circuito ejemplo.*

La **configuración de pines** de Arduino sería:

- Como el detector PIR genera un voltaje al realizar la detección, su señal se llevará a una de las entradas analógicas con las que cuenta Arduino, en este caso la A2.
- El piezoeléctrico será activado a través de una de las salidas digitales, en este caso el pin 4.
- La alimentación de la placa la tomamos directamente de los pines de 5 V y GND que encontramos en la placa de Arduino.

El **código del programa** sería el siguiente:

```
// Definición de variables globales
int piezo = 4;
int pir = 0;

void setup() // Bloque de configuración de las comunicaciones con el exterior
{
pinMode(piezo, OUTPUT); //Como 'piezo' vale 4, se configura el pin 4 como SALIDA
} // Fin del 'setup'

void loop() // Bloque de programa principal
{
pir = analogRead(A2);     // Lee y almacena el valor que está generando el detector
if (pir != 0) { // Comprueba si se ha activado el detector
for (int i=0; i<5; i++) {     // Bucle para repetir la activación/desactivación cinco veces
                digitalWrite(piezo, HIGH);     // Escritura en el pin 4 un nivel ALTO de tensión
               delay(500);     // Parada de programa de 500 milisegundos
               digitalWrite(piezo, LOW);     // Escritura en el pin 4 un nivel BAJO de tensión
               delay(500);
} // Fin del bucle 'for'
} // Fin del condicional 'if'

} // Fin del 'loop'
```

En el enlace https://www.tinkercad.com/things/f50N8kSfmbl se puede comprobar el montaje y su funcionamiento.

Actividad resuelta 2.3

Aviso luminoso por exceso de calor

El sistema controlado por Arduino generará una intermitencia con dos lámparas cuando la temperatura ambiente del local donde se ha instalado sea perjudicial (50 ºC) para el ser humano, previamente (40 ºC) se habrá activado el motor que mueve las aspas de un ventilador, que se desactivará en el momento en que la temperatura disminuya de 25 ºC, o bien, se activen las luces de alarma.

Los **elementos necesarios** para llevar a cabo la actividad son los que se pueden observar en la Figura 2.58.

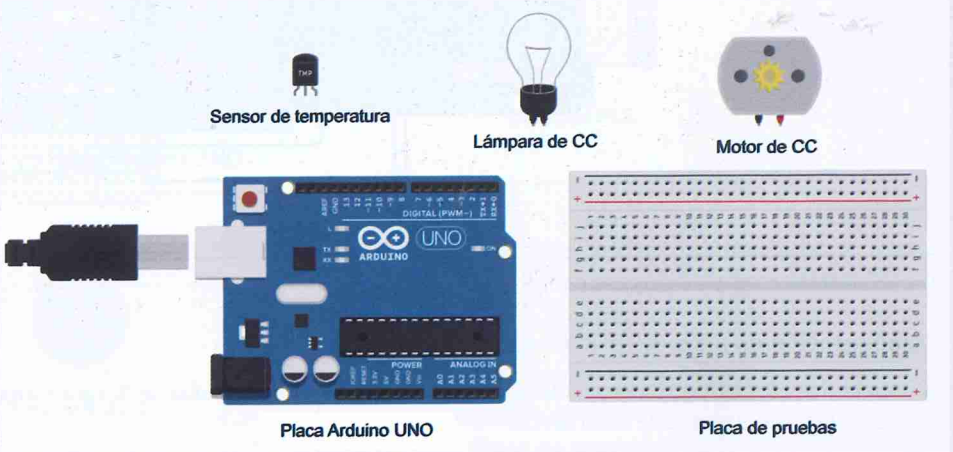


Figura 2.58. *Elementos necesarios para el montaje del circuito ejemplo.*

El **funcionamiento básico** del sensor de temperatura (TMP) sería como sigue:

El sensor puede medir temperaturas entre –40 ºC y 125 ºC, esta fluctuación genera que el sensor en su salida (Vout) genere un valor de voltaje entre los 99,9 mV y los 1,75 V, respectivamente, en estos márgenes.

Este voltaje variará de manera proporcional cuando se modifique el valor de temperatura que detecta.

Su alimentación eléctrica se suministrará desde los pines de 0 a 5 V de Arduino, siendo el voltaje máximo que soporta el sensor de 5,25 V.

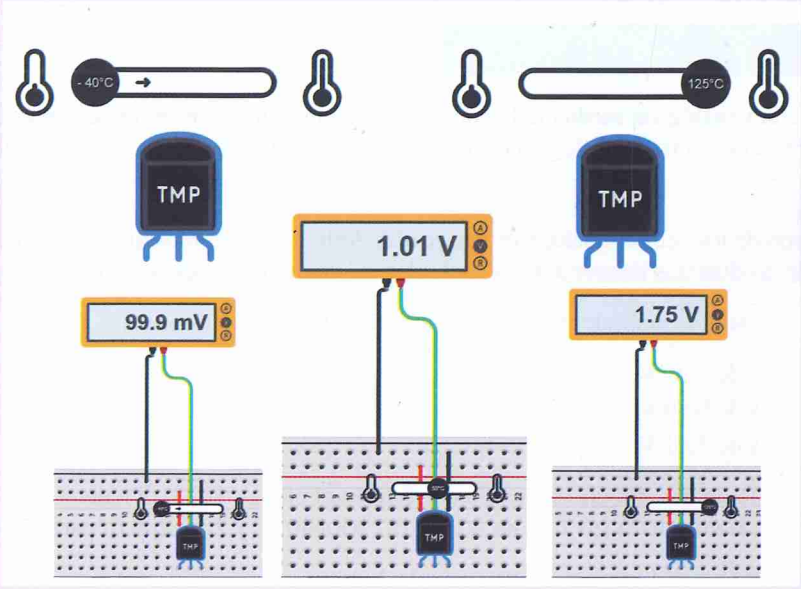


Figura 2.59. *Respuesta del sensor de temperatura y funcionamiento.*

El **montaje** sería el mostrado en la Figura 2.60.

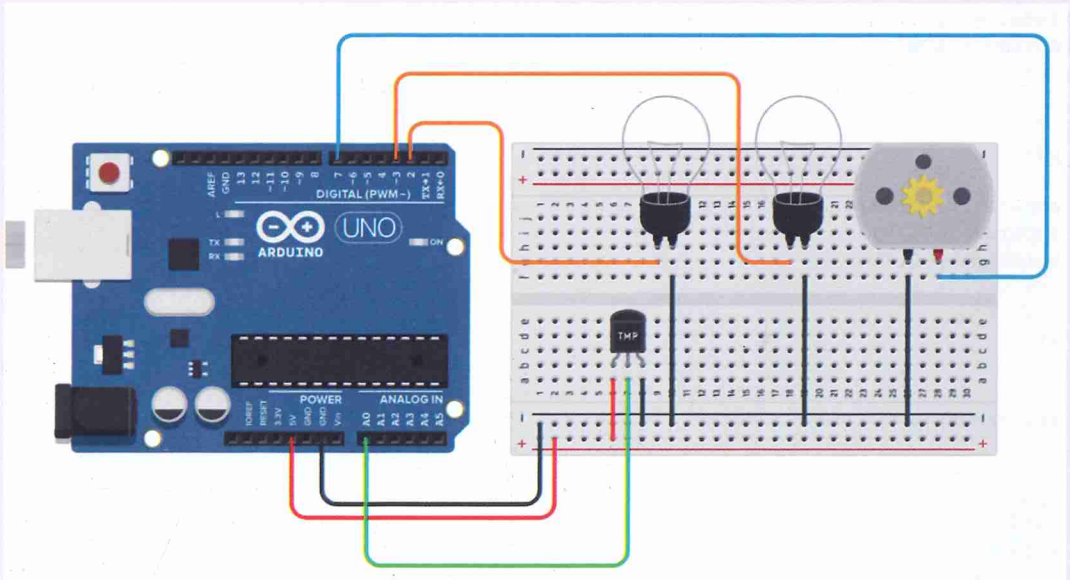


Figura 2.60. *Montaje completo del circuito ejemplo.*

La **configuración de pines** de Arduino sería:

- Como el sensor TMP genera un voltaje al realizar la detección, su señal se llevará a una de las entradas analógicas con las que cuenta Arduino, en este caso la A0.
- El motor del ventilador será activado a través de una de las salidas digitales, en este caso el pin 7. Igual que las **lámparas** que se encuentran en los pines 2 y 3 respectivamente.
- La alimentación de la placa se toma directamente de los pines de 5 V y GND que encontramos en la placa Arduino.

Recuerda:

Arduino realiza una lectura analógica, mediante la conversión de una señal de este tipo en un código digital, el voltaje que se puede suministrar a una entrada analógica es de 0 V a 5 V, que serán decodificados en códigos del 0 al 1023.

Debido a la codificación de los valores analógicos que realiza Arduino, tendremos que observar cuáles son los códigos de los voltajes generados por las distintas temperaturas y umbrales existentes en el enunciado de este ejemplo.

Así, tendremos para los distintos umbrales (datos obtenidos directamente del sensor):

- Para 30 ºC – una salida de 0,79 V.
- Para 40 ºC – una salida de 0,89 V.
- Para 50 ºC – una salida de 1,01 V.

Ahora, mediante una regla de tres directa, sabiendo que 5 V es el código 1023, obtenemos los códigos de los distintos valores de tensión anteriores, siendo 162 (161,6) para 30 ºC, 182 para 40 ºC y 207 (206,6) para 50 ºC.

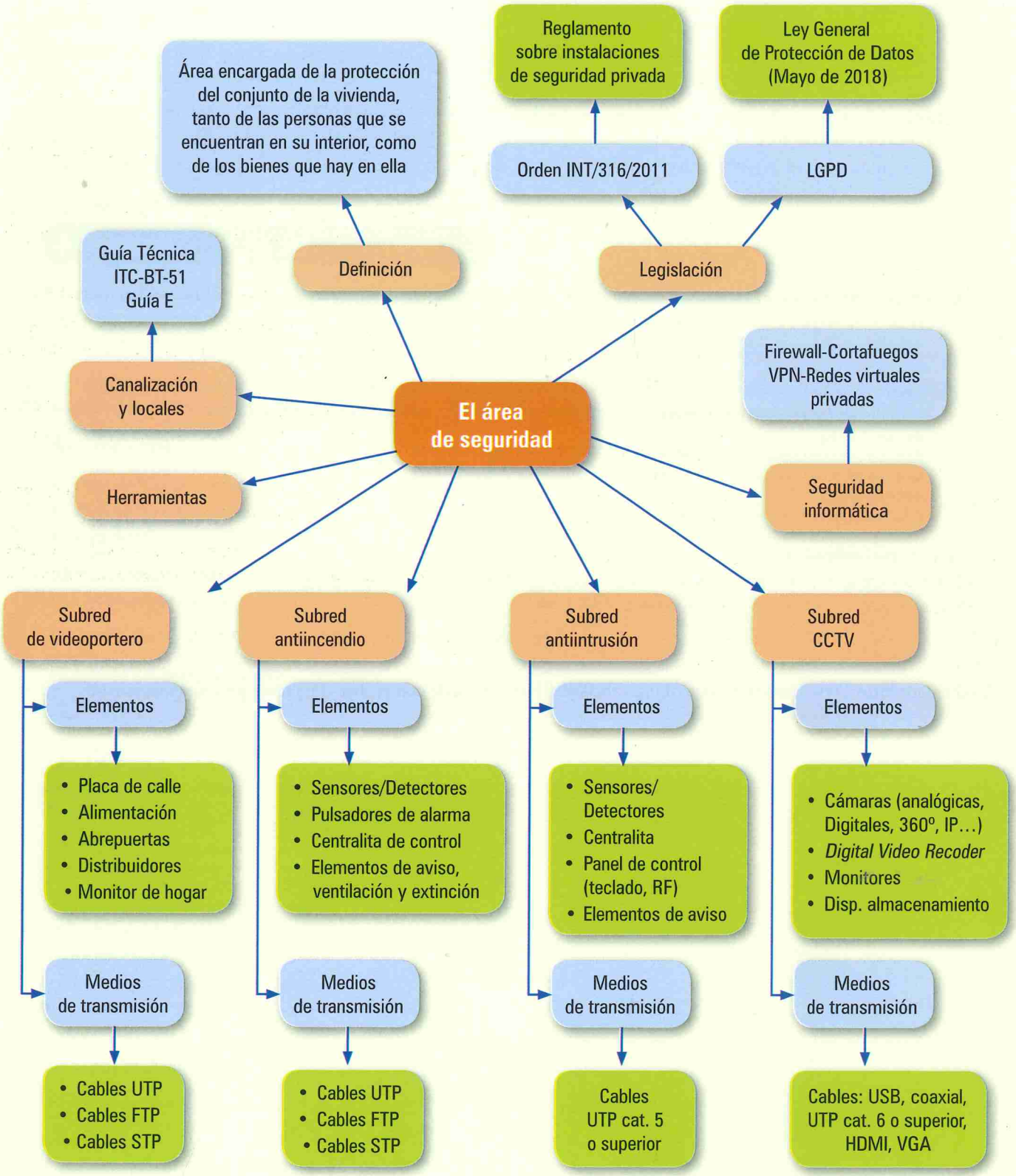
Con estos datos, procedemos a realizar la programación de Arduino.

El **código del programa** sería el siguiente:

```
// Definición de variables globales
int lampara1 = 3, lampara2 = 2;
int ventilador = 7;
bool VentActivo = LOW; // Variable booleana para observar si el ventilador está activado
int TMP = 0; // Variable para almacenar el valor del sensor

// Bloque de configuración de las comunicaciones con el exterior
void setup()
{
pinMode(lampara1, OUTPUT);
pinMode(lampara2, OUTPUT);
pinMode(ventilador, OUTPUT);
} // Fin del código de configuración
// Bloque de programa principal
void loop()
{
// Lee y almacena en la variable TMP el valor que está generando el sensor
TMP = analogRead(A0);

/* Si la temperatura es menor a 25°
y el ventilador está activado, entonces
lo apagamos*/
if ((TMP < 162) && VentActivo) {
VentActivo = LOW;
digitalWrite(ventilador, LOW);
} // Fin if 1
```

```
/* Si la temperatura es mayor de 40°
y menor de 50° el ventilador se activa*/
if ((TMP > 182) && (TMP < 207)) {
VentActivo = HIGH;
digitalWrite(ventilador, HIGH);
} // Fin if 2

/* Si la temperatura es mayor de 50°
desactiva el ventilar para evitar propagación
de incendio y activa las alarmas luminosas*/
if (TMP > 207) {
VentActivo = LOW;
digitalWrite(ventilador, LOW);

/* Genera la intermitencia de lámparas mientras
la temperatura sea superior a 50°, cada lámpara
se enciende 0,5 segundos (500 milisegundos)*/
while (TMP > 207) {
      digitalWrite(lampara1, HIGH);
      delay(500);
      digitalWrite(lampara1, LOW);
      digitalWrite(lampara2, HIGH);
      delay(500);
      digitalWrite(lampara2, LOW);
  // Lee por si se modifica la temperatura ambiente
  TMP = analogRead(A0);
  }
 } // Fin if 3
} // Fin bloque principal LOOP
```

En el enlace https://www.tinkercad.com/things/5N5k4LBHzxr se puede comprobar el montaje y su funcionamiento.



RESUMEN DE CONCEPTOS

- El **área de seguridad** se encarga de ofrecer las herramientas necesarias para garantizar la protección de las personas, los inmuebles y las propiedades que en ellas existan.
- La arquitectura del área de seguridad se engloba dentro de la infraestructura RGCS del hogar digital.
- Legalmente, según la normativa UNE-EN, existen cuatro grados de seguridad, en función de los lugares y bienes que deben proteger.
- En toda la instalación debe seguir el cumplimiento de la Ley General de Protección de Datos (LGPD), vigente desde el 25 de mayo de 2018 en toda Europa.
- Puede contener cuatro subredes que completan las posibilidades existentes de seguridad en el hogar, así estas son: seguridad electrónica, que engloba las subredes antiincendio y antiintrusión y robo; control de acceso y videoporteros y la subred de circuito cerrado de televisión.
- Percibirán su entorno a través de sensores y detectores y modificarán el estado del mismo a través de los actuadores.
- Un detector y un sensor difieren en el tipo de respuesta que aportan al sistema, el sensor aporta en su respuesta una información analógica más precisa, mientras que el detector informa al sistema de si se cumple la premisa de su detección o no, es decir, dará una información digital.
- Se pueden encontrar sistemas pasivos y activos, los sistemas pasivos no generan una solución inmediata a la alerta (CCTV, antiintrusión), sí generan un aviso, mientras que los activos (control de acceso, antiincendio) intentarán, mediante los mecanismos instalados, además de un aviso, dar con la solución a la alerta activada.
- Los CRA, centros de registro de alarmas, son los centros de control de los sistemas de alarmas, controlados generalmente por empresas privadas dedicadas a este sector y que ofrecen los servicios de seguridad.
- Otro aspecto importante a recordar es el de tener los sistemas de seguridad informática siempre actualizados, ya que el sistema estará conectado a internet a través de la pasarela, lo que permitirá a *hackers* y *crackers* tener la posibilidad de acceder e incluso sabotear la instalación.
- Existen elementos de programación que pueden ser utilizados para crear sistemas de alarma sin necesidad de tener una centralita como tal en el hogar. Estos pueden ser autómatas y microcontroladores.

Actividades de comprobación

2.1. Indica si las siguientes afirmaciones son verdaderas (V) o falsas (F).

- La seguridad electrónica solo se utiliza para proteger propiedades. ☐
- La radiofrecuencia es un sistema de comunicación en instalaciones de hogar digital. ☐
- Cuando hay una cámara de seguridad en una instalación protegida, debe estar advertido para cumplir la LGPD. ☐
- Los establecimientos obligados a tener sistema de seguridad son los de grado 3. ☐
- Precisión es el error máximo esperado al realizar varias veces la misma medida. ☐
- Los sensores surgen ante la necesidad de imitar los sentidos humanos de manera eléctrica. ☐
- El grado 0 de seguridad no está incluido en la graduación marcada por las normas UNE-EN. ☐
- La precisión de un sensor es el error de medida mínimo esperado. ☐
- Un detector de doble tecnología se basa en el empleo simultáneo de un detector infrarrojos y un sensor de movimiento. ☐
- Un lector de retina es un tipo de sensor biométrico. ☐
- El término pasarela se aplica al elemento que comunica nuestro hogar digital con el mundo exterior. ☐
- La base del hogar digital es que todo esté bajo el control de una central. ☐
- La sensibilidad es la mínima variación en la entrada, que produce un cambio en la salida del sensor. ☐
- Un termorresistor es un sensor activo. ☐
- Un detector provoca varios niveles en su salida, dependiendo de las percepciones de entrada que recibe. ☐
- La sensibilidad en cámaras es la cantidad de luz mínima (visible y/o infrarroja) que permite ver la imagen obtenida con calidad. ☐
- Un termopar es un detector activo. ☐
- Los sensores son elementos que utiliza el sistema para modificar el estado en equipos e instalaciones. ☐

2.2. El objetivo general del área de seguridad es:

- **a)** Dotar al usuario la manera de controlar de forma remota las incidencias relativas a la seguridad de personas y bienes.
- **b)** Dotar a la vivienda o local la manera de controlar de forma remota las incidencias relativas a la seguridad de personas y bienes.
- **c)** Dotar a las CRA la manera de controlar de forma remota las incidencias relativas a la seguridad de personas y bienes.
- **d)** Ninguna de las respuestas anteriores es correcta.

2.3. Un termopar es:

- **a)** Un sensor pasivo.
- **b)** Un sensor activo.
- **c)** No es un sensor.

2.4. Los principales sistemas de comunicación de los sistemas del hogar digital son:

- **a)** Por bluetooth.
- **b)** Por wifi.
- **c)** Por radiofrecuencia.
- **d)** Por cable.
- **e)** Todas las respuestas anteriores son correctas.
- **f)** Ninguna de las respuestas anteriores es correcta.

2.5. Una LDR (*Light Dependent Resistor*) es:

- **a)** Un sensor pasivo.
- **b)** Un sensor activo.
- **c)** No es un sensor.

2.6. La principal diferencia entre un sensor y un detector es:

- **a)** No poseen la misma capacidad de recepción de las magnitudes.
- **b)** El tipo de señal que dan como respuesta a la recepción de las magnitudes.
- **c)** Es indistinto su uso, así que las diferencias no son representativas en este tipo de instalaciones.
- **d)** Ninguna de las respuestas anteriores es correcta.

2.7. ¿Cuál es la persona o entidad que se encarga de supervisar, asesorar, tramitar las reclamaciones, colaborar con las autoridades de cada país y supervisar las nuevas tecnologías que pueden tener una incidencia en la protección de datos?

a) El encargado del departamento internacional de la empresa suministradora de servicios.

b) Los indicados de manera específica en la LGPD aprobada el pasado 25 de mayo de 2018.

c) El SEPD (supervisor europeo de protección de datos).

d) Ninguna de las respuestas anteriores es correcta.

Actividades de aplicación

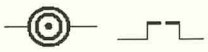
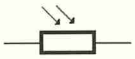
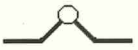
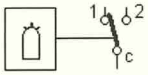
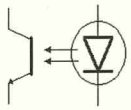
2.8. Expón y explica claramente los grados de las instalaciones de seguridad que aparecen expuestos en las normas UNE-EN.

2.9. Explica cuáles son las características técnicas de los sensores.

2.10. Enumera los tipos de verificación existentes ante la recepción de una alarma.

2.11. ¿Qué es el panel de control de un sistema de seguridad electrónica? ¿Cuáles son sus características?

2.12. En el siguiente ejercicio, relaciona cada símbolo expuesto a la izquierda con el elemento correspondiente de la columna de la derecha.

Símbolo	Elemento
	• Micrófono
	• Termistor activo
	• Sensor de gas
	• Cámara a color
	• Cámara en B/N
	• Detector de líquidos
	• Resistor dependiente de la luz
	• Optoacoplador
	• Detector de tacto
	• Detector de apertura de puerta

2.13. Indica las funcionalidades del DVR para unificar las señales recibidas de las cámaras, sus características y funcionamiento.

2.14. Define los siguientes conceptos:

a) Central procesadora.

b) Gabinete de sirena exterior.

c) Sensor sísmico.

d) Detector de movimiento.

2.15. ¿Cuáles son las lentes más comunes entre las cámaras de videovigilancia?

2.16. Clasifica los tipos de tarjetas que se suelen utilizar en los sistemas de control de acceso.

2.17. ¿Qué requisitos debe cumplir una instalación para estar legalmente cubierta?

2.18. ¿Qué es un DVR? Explica las funciones que puede realizar en las instalaciones donde se coloca.

2.19. ¿A qué preguntas debe responder una instalación de CCTV para asegurar que es correcta?

2.20. ¿Qué ventajas ofrece la alimentación por cable PoE?

Actividades de ampliación

2.21. A lo largo de la unidad, son varias veces las que se ha indicado la existencia de empresas privadas que se dedican a la instalación, verificación y control de sistemas de seguridad en el hogar digital. Se pide:

- Realizar una lista con las empresas locales o provinciales que se encargan de ofrecer este tipo de servicios.
- Realizar un estudio y presentarlo en clase de los servicios que ofrecen cada una.
- Realizar una clasificación de aquellas que, bajo el criterio del alumno, sean las mejores por la calidad de los servicios y la crítica social que reciben.

2.22. Estudio de campo.

- De las empresas de seguridad que existen en el entorno local del centro escolar, hacer la elección de una de ellas para realizar una visita técnica con el/la profesor/a de la asignatura.
- Para la elección de la empresa se crearán grupos, de no más de cuatro miembros, para realizar una entrevista a las distintas empresas (una por grupo).
- La entrevista deberá centrarse en los servicios que ofrecen hacia el hogar digital.
- Tras la entrevista, poner en común en clase los resultados obtenidos, sacar conclusiones y programar la visita a la empresa mejor valorada por el alumnado tras la presentación.

2.23. Uso de Arduino.

- Utilizando la plataforma Tinkercad, y con el soporte de Arduino, crear el siguiente prototipo de sistema de detección de gas.
- Contaremos con un detector de gas, situado en un lugar donde puede crearse cierta acumulación y puede llegar a ser peligroso.
- Tras la detección de este gas durante 30 segundos, comenzará a moverse un ventilador para intentar extraer la acumulación del mismo.

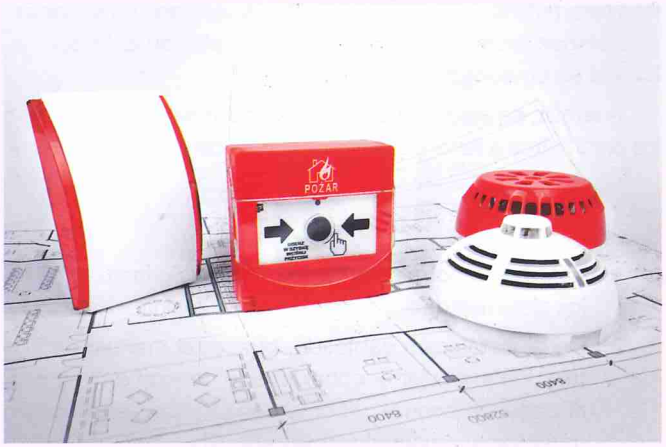
  Si tras 1 minuto este sigue detectando, se activará un segundo ventilador.

  Si pasados 3 minutos no ha dejado de detectar, se activará una alarma visual y auditiva mediante una lámpara y un piezoeléctrico a la vez y de manera intermitente mientras no descienda el nivel de gas ambiente.

2.1. Instalación de un sistema antiincendios

Utilizando los dispositivos antiincendio con los que se cuenta en el laboratorio, se pretende que con esta práctica y los conocimientos adquiridos en unidades anteriores montar una pequeña instalación de un sistema de seguridad antiincendios.

Además, estudiaremos las normas de instalación, así como los parámetros a tener en cuenta a la hora de efectuar la misma.



✓ Se pide:

1. Estudiar la normativa de instalación y canalización de los sistemas de alarma en sistemas antiincendios.
2. Buscar el manual de instalación y dibujar el conexionado general en la placa de cómo deben ir los sensores y/o detectores conectados a la centralita.
3. Observar la conexión de los sensores con los que se cuenta en el panel. Dibujar la configuración actual.
4. Conectar aquello que se encuentre mal puesto según el manual y a continuación conectar y poner en marcha el sistema.
5. Exponer diez posibles averías de dispositivos o mal funcionamiento, que debemos tener en cuenta a la hora de conectar un sistema de alarma.
6. Realizar un manual de instalación, donde de manera resumida se expongan los pasos y conexiones que debería tener en cuenta un instalador a la hora de realizar esta instalación.
7. Realizar un manual para que el usuario de la instalación comprenda los pasos que debe cumplir para un correcto funcionamiento de su instalación, para ello nos basaremos en la instalación que se está trabajando.
8. Realizar un pequeño estudio de las empresas que en la actualidad se encargan de este tipo de instalaciones.
9. Hacer una reflexión sobre la utilidad de la práctica.

Informe final

Con todos los datos recopilados anteriormente y una vez revisadas las labores prácticas por el docente, se debe crear un informe con los siguientes apartados:

a) Portada.
b) Enunciado suministrado impreso.
c) Esquema.
d) Memoria de funcionamiento:
   i. Conceptos teóricos en los que se basa la realización de la práctica y que no estén incluidos en las cuestiones propias de la práctica.
   ii. Aspectos prácticos, es decir, ¿qué se ha hecho?, ¿cómo se ha hecho?, ¿por qué se hace así? (esto es, una relación entre los conceptos teóricos y la práctica realizada).
   iii. ¿Para qué nos sirve lo que estamos realizando?
   iv. Cálculos si fuesen necesarios y que no están incluidos en las cuestiones.
e) Cuestionario.
f) Conclusiones personales tras la realización práctica.
g) Lista de componentes y presupuesto.
h) Anexos y pliego de condiciones.

2.2. Instalación de un sistema de seguridad antiintrusión

Con esta práctica y los conocimientos adquiridos en la unidad, se pretende montar y comprobar una instalación antirrobo cableada de un sistema de seguridad.

Además, se estudiará la normativa de instalación, así como los parámetros a tener en cuenta a la hora de efectuar la misma.

✓ Se pide:

1. Estudiar la normativa de instalación y canalización de los sistemas de alarma en sistemas antiintrusión y robo.
2. De la instalación cableada, buscar el manual de instalación y dibujar el conexionado general en la placa, el panel de control, y cómo deben ir los sensores y/o detectores conectados a la centralita.
3. Si ya está montado, observar la conexión de los sensores con los que se cuenta en el panel. Dibujar la configuración actual.
4. Conectar aquello que se encuentre mal puesto según el manual o no esté conectado y, a continuación, poner en marcha el sistema.
5. Exponer diez posibles averías de dispositivos o mal funcionamiento, que debemos tener en cuenta a la hora de conectar un sistema de alarma.
6. Realizar un manual de instalación, donde de manera resumida se expongan los pasos y conexiones que debería tener en cuenta un instalador a la hora de realizar esta instalación.
7. Realizar un manual para que el usuario de la instalación comprenda los pasos que debe cumplir para un correcto funcionamiento de su instalación, para ello nos basaremos en la instalación que se está trabajando.
8. Realizar un estudio de las empresas que en la actualidad se encargan de este tipo de instalaciones en el entorno local o provincial.

Informe final

Con todos los datos recopilados anteriormente y una vez revisadas las labores prácticas por el docente, se debe crear un informe con los siguientes apartados:

a) Portada.
b) Enunciado suministrado impreso.
c) Esquema.
d) Memoria de funcionamiento:
   i. Conceptos teóricos en los que se basa la realización de la práctica y que no estén incluidos en las cuestiones propias de la práctica.
   ii. Aspectos prácticos, es decir, ¿qué se ha hecho?, ¿cómo se ha hecho?, ¿por qué se hace así? (esto es, una relación entre los conceptos teóricos y la práctica realizada).
   iii. ¿Para qué nos sirve lo que estamos realizando?
   iv. Cálculos si fuesen necesarios y que no están incluidos en las cuestiones.
e) Cuestionario.
f) Conclusiones personales tras la realización práctica.
g) Lista de componentes y presupuesto.
h) Anexos y pliego de condiciones.

2.3. Instalación de un sistema de seguridad antiintrusión inalámbrico

Con esta práctica y los conocimientos adquiridos en la unidad, se pretende configurar los dispositivos de una instalación antirrobo o antiintrusión inalámbrica.

✓ Se pide:

1. Estudiar la instalación del sistema y exponer cómo debe realizarse, acompañándola con gráficos de conexión.
2. Observar los detectores que acompañan a la central de alarma y explicar el funcionamiento de los mismos.
3. Ponerla en funcionamiento y explicar cómo debe realizarse.
4. Realizar un breve manual de usuario de este sistema. Se debe recordar cómo se usa, no cómo se instala.
5. Hacer una reflexión sobre la utilidad de la práctica.

Informe final

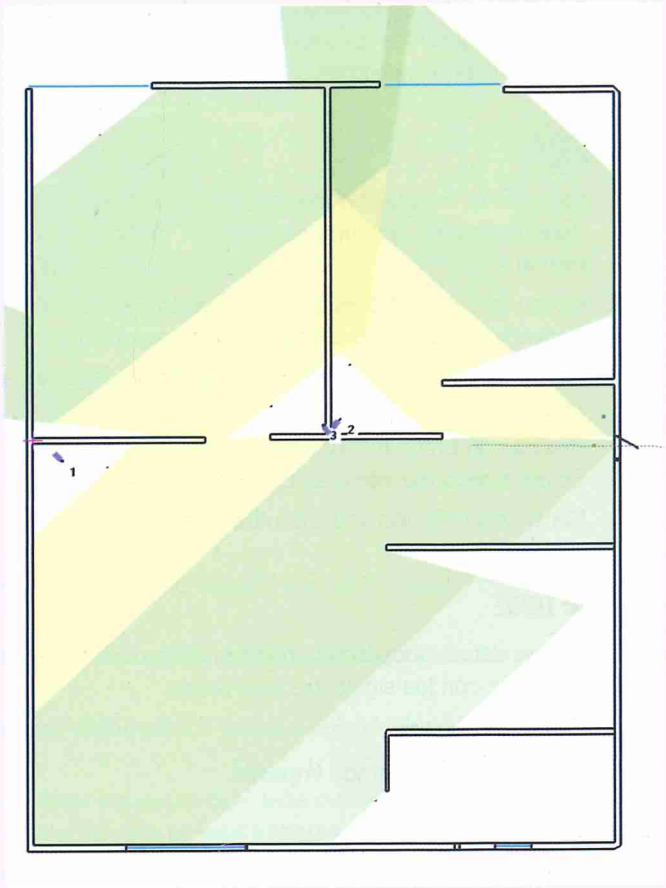
Con todos los datos recopilados anteriormente y una vez revisadas las labores prácticas por el docente de laboratorio, se debe crear un informe con los siguientes apartados:

a) Portada.
b) Enunciado suministrado impreso.
c) Esquema.
d) Memoria de funcionamiento:
   i. Conceptos teóricos en los que se basa la realización de la práctica y que no estén incluidos en las cuestiones propias de la práctica.
   ii. Aspectos prácticos, es decir, ¿qué se ha hecho?, ¿cómo se ha hecho?, ¿por qué se hace así? (esto es, una relación entre los conceptos teóricos y la práctica realizada).
   iii. ¿Para qué nos sirve lo que estamos realizando?
   iv. Cálculos si fuesen necesarios y que no están incluidos en las cuestiones.
e) Cuestionario.
f) Conclusiones personales tras la realización práctica.
g) Lista de componentes y presupuesto.
h) Anexos y pliego de condiciones.

2.4. Diseño de una instalación de circuito cerrado de televisión

Práctica de toma de contacto con el software IP Video Design, para diseñar instalaciones de circuito cerrado de TV en viviendas y locales. Se puede encontrar el enlace para descargarlo en las páginas web que se indican al final de la unidad (se debe recordar que es una versión de prueba de 30 días).

Además de estudiar las normas de instalación, así como los parámetros a tener en cuenta a la hora de efectuar la misma, desarrollaremos un proyecto de una instalación de CCTV para el aula-taller.



✓ Se pide:

1. Estudiar la normativa de instalación y canalización de los sistemas de alarma en sistemas de videovigilancia y realizar un resumen de la misma.
2. Crear un proyecto nuevo con el software indicado, realizar un plano del aula-taller de telecomunicaciones en el que se trabaja normalmente.
3. Realizar la instalación de manera que quede totalmente protegida y vigilada con nuestro sistema de CCTV y sacar las conclusiones oportunas de por qué se realiza así.
4. Realizar las capturas de pantalla oportunas para que la memoria quede completamente asesorada. Introducir personas y objetos para la completa comprobación.
5. Guardar y enviar el proyecto por correo electrónico al docente del aula de laboratorio.

Informe final

Con todos los datos recopilados anteriormente y una vez revisadas las labores prácticas por el docente de laboratorio, se debe crear un informe con los siguientes apartados:

a) Portada.
b) Enunciado suministrado impreso.
c) Esquema.
d) Memoria de funcionamiento:
   i. Conceptos teóricos en los que se basa la realización de la práctica y que no estén incluidos en las cuestiones propias de la práctica.
   ii. Aspectos prácticos, es decir, ¿qué se ha hecho?, ¿cómo se ha hecho?, ¿por qué se hace así? (esto es, una relación entre los conceptos teóricos y la práctica realizada).
   iii. ¿Para qué nos sirve lo que estamos realizando?
   iv. Cálculos si fuesen necesarios y que no están incluidos en las cuestiones.
e) Cuestionario.
f) Conclusiones personales tras la realización práctica.
g) Lista de componentes y presupuesto.
h) Anexo y pliego de condiciones.

2.5. Instalación de un circuito cerrado de televisión

Utilizando el material de CCTV disponible en el laboratorio, se pretende tener una toma de contacto con los elementos que componen las instalaciones de CCTV y los medios de transmisión entre los mismos, mediante la instalación de un circuito cerrado de televisión local.

✓ Se pide:

1. Estudiar y realizar un resumen de la Ley General de Protección de Datos en lo referente a los CCTV.
2. Realizar un estudio de las características que tienen las cámaras utilizadas en los sistemas de circuitos cerrados de televisión.
3. Exponer los distintos elementos que se encargan de unificar las señales de vídeo obtenidas por las cámaras para poder visionarlas o grabarlas.
4. Con los elementos suministrados en clase, realizar una instalación local de CCTV. Especificar el resultado obtenido. Tras esto, unirse a otro grupo de trabajo del taller e instalar dos cámaras en un único DVR. Explicar las diferencias observadas entre las dos instalaciones. Apagar las luces del local para ver qué ocurre.
5. Realizar un dibujo del panel de conexiones del DVR. Exponer los tipos de conectores que encuentran, así como las características técnicas más importantes de las señales que se obtienen.
6. Buscar las características técnicas de las cámaras utilizadas y realizar un resumen con los datos obtenidos.
7. Hacer una reflexión de la utilidad de esta práctica.

Informe final

Con todos los datos recopilados anteriormente y una vez revisadas las labores prácticas por el docente de laboratorio, se debe crear un informe con los siguientes apartados:

a) Portada.
b) Enunciado suministrado impreso.
c) Esquema.
d) Memoria de funcionamiento:
   i. Conceptos teóricos en los que se basa la realización de la práctica y que no estén incluidos en las cuestiones propias de la práctica.
   ii. Aspectos prácticos, es decir, ¿qué se ha hecho?, ¿cómo se ha hecho?, ¿por qué se hace así? (esto es, una relación entre los conceptos teóricos y la práctica realizada).
   iii. ¿Para qué nos sirve lo que estamos realizando?
   iv. Cálculos si fuesen necesarios y que no están incluidos en las cuestiones.
e) Cuestionario.
f) Conclusiones personales tras la realización práctica.
g) Lista de componentes y presupuesto.
h) Anexo y pliego de condiciones.

Enlaces web de interés

- Agencia Española de Protección de Datos:
  https://www.aepd.es
- European Data Protection Supervisor:
  https://europa.eu/european-union/index_es
- Orden INT/314/2011, de 1 de febrero, sobre empresas de seguridad privada:
  https://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-3168
- Orden INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada:
  http://www.interior.gob.es/web/servicios-al-ciudadano/normativa/ordenes-int/orden-int-316-2011-de-1-de-febrero
- Orden INT/1504/2013, de 30 de julio, sobre modificación de ciertos aspectos de la anterior ley sobre seguridad privada:
  https://www.boe.es/eli/es/o/2013/07/30/int1504
- Última ley sobre seguridad privada en España sobre personal y servicios:
  https://www.boe.es/buscar/doc.php?id=BOE-A-2014-3649
- Ministerio del Interior, servicios al ciudadano sobre centrales de alarma:
  http://www.interior.gob.es/web/servicios-al-ciudadano/seguridad/medidas-de-seguridad-en-entidades-y-establecimien/centrales-de-alarmas
- Agencia Española de Protección de Datos. Videovigilancia:
  https://www.aepd.es/areas/videovigilancia/index.html
- Guía de videovigilancia de la Asociación Española de Protección de Datos:
  https://www.aepd.es/media/guias/guia-videovigilancia.pdf
- Software para arquitectura, ingeniería y construcción:
  http://itcalc.cype.es/
- Aplicación para el diseño de sistemas de CCTV (de pago, con período de prueba de 30 días):
  http://www.jvsg.com/ip-video-system-design-tool/
- Aplicación para diseño de sistemas de CCTV (gratuita):
  https://www.hanwhasecurity.com/wisenet-tool-box/
- Laboratorio de electrónica online, incluye Arduino (requiere registro, gratuita):
  www.tinkercad.com

Páginas gratuitas de recursos de presentación (todas ellas necesitan registro):

- Recurso Genial.ly para presentaciones:
  https://www.genial.ly/es
- Recurso Kahoot para crear juegos educativos:
  https://kahoot.com/
- Recurso Prezzi para crear presentaciones interactivas:
  https://prezi.com