

1. Equipos y elementos de CCTV y seguridad electrónica.



Caso práctico

Si conoces el funcionamiento de los sistemas de seguridad, te habrás preguntado como es posible que los aparatos detecten a las personas en la oscuridad o a personas que quieran entrar en un local cerrado antes de que accedan al mismo. También te estarás planteando como se puede alertar en tan poco tiempo a la policía cuando se produce un robo, incluso en el mismo momento que están produciendo.



Un estudiante que esté acabando su formación debe saber bastante de todo esto ya que lo habrá estudiado recientemente y conocerá las tecnologías empleadas en los sistemas antirrobo.

La instalación de estos sistemas de seguridad para la prevención de robos, hurtos, incendios y hechos de vandalismo debe comenzar analizando los riesgos.

Lo normal de cualquier persona que empieza a estudiar algo nuevo es que tenga curiosidad por lo que va a estudiar y que se plantee una gran cantidad de preguntas. Esa curiosidad es buena y en nuestro caso no debe ser diferente, curiosidad por saber cómo funcionan los diferentes dispositivos y curiosidad por saber que vas a estudiar.

En este tema vas a aprender a identificar los **diferentes tipos de riesgos** a los que estamos expuestos y los equipos que forman parte de los sistemas de seguridad y los CCTV, conociendo las características más importantes y las partes de estos elementos.

Para tener una primera definición, diremos que un **sistema de seguridad** es el conjunto de elementos y de las instalaciones necesarias para proporcionar a las personas y bienes materiales una protección frente a robos, atracos, hurtos y como no, incendios.

Podemos hacer una primera **clasificación de los sistemas de seguridad**.

Clasificación de los sistemas de seguridad

Tipos de sistemas	Elementos básicos
Robo y atraco	Sensores y centrales de alarma. Aviso a C.R.A. Señalización del robo. Dispositivos de acceso. CCTV. Aviso a C.R.A.
Incendio	Sensores y centrales de incendios. Aviso a C.R.A. Accionamiento de dispositivos de extinción de incendios, dispositivos de aviso y señalización. Alumbrado de emergencia. Asimismo habrá extinción manual, bocas de incendio.
Antiintrusion y antihurto	Protección de los artículos de los comercios. Escáner de Rayos X. Detectores de explosivos, arco detectores de metales y etiquetas activas/pasivas.
Alarmas técnicas especiales	Detectores: de metales, de humedad, de sustancias químicas, de presión, de gas, de temperatura, sonda de nivel de líquidos.



Para saber más

El siguiente enlace puede resultar muy interesante para conocer nuevos productos de seguridad y noticias relacionadas con todos estos sistemas y elementos.

 [Elementos de seguridad.](#)



Materiales formativos de FP Online propiedad del Ministerio de Educación y Formación Profesional.

[Aviso Legal](#)

1.- Riesgo.



Caso práctico

Isidro sabe que para montar una instalación de seguridad y protegernos frente a robos, o incendios tiene que empezar por realizar un estudio de los riesgos a los que nos enfrentamos y de la instalación a proteger.



Los **sistemas de seguridad** están cada día más extendidos. Actualmente se utilizan en hogares, pequeños negocios, industrias o lugares de alto riesgo como bancos, joyerías, centrales nucleares. Además protegen a las personas.

En un principio el sistema de seguridad detectará un riesgo, por ejemplo, incendio o robo, luego lo señalará y por último iniciará las acciones encaminadas a evitar, disminuir o extinguir los peligros.

Un sistema de seguridad no debe proporcionar falsas alarmas ya que en la práctica además de no ser seguro, tiende a ser ignorado.

Podemos definir un **Riesgo** como la  probabilidad de que ocurra un evento, fortuito o intencionado desencadenando un peligro con consecuencias importantes (lesiones a las personas, daño a los equipos, medioambientales, de interrupción de una actividad).

También sabemos que **a mayor vulnerabilidad mayor riesgo** y, por tanto, **mayor probabilidad de**  peligro. Podemos realizar una primera clasificación en función del tipo de riesgo que queremos evitar.

Los 4 grandes bloques de aplicación de los riesgos son:

1. De robo e intrusión.
2. De incendio.
3. Vigilancia de procesos industriales.
4. Vigilancia de clientes y empleados.

Para intentar dar respuesta a estos tipos de riesgos tenemos: sistemas anti  intrusión, circuitos cerrados de televisión con  video vigilancia, controles de acceso, centrales de detección de fuego y sistemas de extinción de incendios, centrales receptoras de alarmas y luces de emergencia entre otros.

El riesgo se puede evitar o disminuir dependiendo de las **medidas** que tomemos. Este es un ejemplo, elimina un factor y eliminarás el fuego.





Para saber más

En este enlace tienes información de lo que es el robo, y los elementos que intervienen así como la regulación del robo en España.

 [Definición del robo en España.](#)

En este enlace te explican la definición de riesgo con aclaraciones importantes.

 [Definición de riesgo.](#)

1.1.- Análisis de riesgo.



Caso práctico

Isidro cuando empezó a estudiar este módulo se planteaba las siguientes cuestiones. ¿Cómo se pueden evaluar los riesgos y reducirlos? ¿Qué es lo que debemos saber?



A la hora de **analizar un riesgo** debemos plantearnos varias **preguntas**:

- ✓ ¿Qué se necesita proteger?
- ✓ ¿De quién debe ser protegido?
- ✓ ¿En qué entorno se encuentran dichos objetos?
- ✓ ¿Qué valor tiene lo que vamos a proteger?
- ✓ ¿Qué reglamentación existe al respecto?

Haremos un **estudio de valoración del riesgo** en función de la probabilidad y  **gravedad**, entendiéndolas como el accidente más probable o habitual.

¿Cómo vamos a realizar la evaluación de riesgos?

Tendremos que identificar las posibles **amenazas, vulnerabilidades y probabilidad** de que ocurra en relación con nuestros activos. Así mismo, tendremos que disponer de normas para la aceptación del riesgo y fijar los niveles de riesgo mínimos.

Por lo tanto, a la hora de **identificar los riesgos** tendremos que tener en cuenta:

1. La evaluación de los riesgos. Es decir, identificar los posibles riesgos en base a lo que queramos proteger.
2. El tratamiento de los riesgos. Determinar que acciones vamos a realizar para evitar los riesgos y en que orden.
3. Fijar los niveles mínimos de riesgo aceptables.

Una vez realizada la instalación, realizaremos un **análisis del cumplimiento de los objetivos marcados** en base a estos criterios de manera que porcentajes altos de cumplimiento signifiquen grados bajos de riesgo y viceversa, es decir, porcentajes bajos de cumplimiento de objetivos significan un grado alto de riesgo.



Para saber más

El siguiente enlace puede resultarte muy interesante para conocer varios conceptos en el campo de la legislación, contempla aspectos referidos a la autorización para crear empresas de seguridad, así como las características de las medidas de seguridad físicas y electrónicas.

 [Legislación sobre la creación de empresas de seguridad.](#)

 [Ley 5/2014, de 4 de abril, de Seguridad Privada.](#)

En el siguiente enlace tienes más información sobre el análisis de riesgos, y los elementos a tener en cuenta.

 [NTP sobre los análisis de riesgo.](#)

1.2.- Niveles de riesgo.



Caso práctico

Silvia, Isidro y su amiga discuten sobre la importancia que tiene hacer una correcta evaluación de los niveles de riesgo antes de iniciar cualquier instalación de seguridad.



Las instalaciones deben de cumplir uno de los cuatro niveles de seguridad en función del grado de riesgo del área protegida según esta recogido en la norma UNE EN 50131-1, orden INT/316/2011, de 1 de febrero, sobre funcionamiento de **los sistemas de alarma en el ámbito de la seguridad privada**:

- ✓ **Nivel 1. De bajo riesgo**, para instalaciones de alarma que tienen señalización acústica y de instalación personal. No se conectan a una central de alarmas (bricolaje).
- ✓ **Nivel 2. De riesgo medio**, utilizado para viviendas y pequeños establecimientos, comercios e industrias que se conectan a un centro de control o central de alarmas. Es el mínimo para sistemas conectados a la policía.
- ✓ **Nivel 3. De riesgo medio/alto**, este nivel cubrirá la mayoría de instalaciones. Destinado a establecimientos obligados a tener medidas de seguridad, así como instalaciones industriales a las que por su actividad se les obligue a disponer de centrales de alarmas, por ejemplo, joyerías, particulares con artículos valiosos o empresas de fabricación de armamento.
- ✓ **Nivel 4. De riesgo elevado**, los requisitos para este nivel son extremadamente especializados. Serán muy pocas instalaciones. Son instalaciones militares, establecimientos que almacenan material explosivo reglamentado, empresas de seguridad con depósito de efectivo y materias peligrosas.

Normativa a aplicar en un local a proteger:

EN 50131-1: sistemas de alarma.

EN 50132: CCTV

EN 50133: Control de accesos.

EN 50134-1: Sistemas de alarma social.

EN 50131-4: Sirenas y señalización.

EN 50131-7: Guías de aplicación.

El **instalador** garantizará que la instalación de un sistema de grado adecuado cumpla con el reglamento regulador de instalación y mantenimiento de equipos y sistemas de telecomunicación, aprobado en el Real Decreto 244/2010 de 5 de marzo.

También podemos **clasificar los niveles de riesgo en función de las distintas zonas a proteger**. Debemos tener en cuenta:

1. La zona **perimetral** del lugar a proteger.
2. Las zonas de acceso al lugar a proteger.
3. La zona concreta que más protección requiere.

Comenzaremos por proteger la **periferia**, es decir, vallas, suelos, ventanas, balcones y cualquier área perimétrica en general. Para esto utilizaremos detección infrarroja, **ultrasonidos**, detección magnética y circuitos cerrados de televisión.

En segundo lugar **los accesos**, es decir, pasillos, puertas, ascensores, elevadores y para ello utilizaremos detectores de **microondas**, ultrasonidos, fotoeléctricos y contactos magnéticos

Y después para la **zona principal** que se quiere proteger podremos utilizar detectores de vibración o de **infrasonidos** junto a algunos de los anteriores.



Para saber más

En el siguiente enlace tienes la normativa relacionada, la Orden INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada:

 [Orden INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada.](#)

En este enlace podemos descargar un interesante archivo con información acerca de los criterios del riesgo de incendios.

 [Criterios del riesgo de incendios.](#) (0.22 MB)



Autoevaluación

¿En cuántas áreas podemos dividir el edificio a proteger?

- Solamente una zona principal.
- Son dos las zonas utilizadas, la periférica y la de acceso.
- Son tres las zonas, la perimetral, la zona de acceso y la zona principal.
- Ninguna de las anteriores.

No es correcta, deberías repasar.

La respuesta no es correcta.

Muy bien, tienes claros los conceptos.

Incorrecta.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

1.3.- Normativa de aplicación.



Caso práctico

Un amigo de **Valle** le pregunta acerca de la normativa que rige las instalaciones de seguridad. Como Valle está informada de las Leyes y Normativas en vigor le contesta que es muy importante conocer la normativa que se aplica para poder defender sus derechos, pero siempre dentro del cumplimiento de la Ley.



En el plano normativo que regula la seguridad privada, la **Ley 5/2014, de 4 de abril, de Seguridad Privada** en su **artículo 5**, y el Reglamento de Seguridad Privada, aprobado por **Real Decreto 2364/1994**, de 9 de diciembre, en su **artículo 1**, atribuye exclusivamente a las **empresas de seguridad** “la instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad”. El artículo 39 del Reglamento de Seguridad Privada, establece que “únicamente podrán realizar las operaciones de instalación y mantenimiento de sistemas de seguridad electrónicos contra robo e intrusión y contra incendios las empresas autorizadas, no necesitando estar inscritas cuando se dediquen sólo a la prevención de la seguridad contra incendios”.

Esto quiere decir que las instalaciones deberán ser realizadas siempre por empresas autorizadas en los siguientes casos:

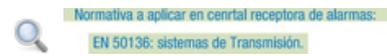
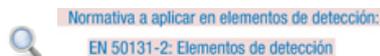
- Que se trate de aparatos o dispositivos electrónicos destinados a tomar medidas de protección física o de cualquier otro tipo.
- Que el objeto de su instalación sea la prevención contra el robo o la intrusión.
- Que la activación de tales aparatos o dispositivos sea susceptible de producir intervención policial, independientemente de que el sistema de seguridad se encuentre o no conectado a una central de alarmas.

También tendremos que tener siempre en consideración las siguientes Leyes y Normativas.

Ley Orgánica 4/1997 de 4 de agosto, que regula la utilización de vídeo cámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

Normas UNE EN 23033, UNE EN 23034 nos documentan sobre como deben ser las señales de evacuación y seguridad. REBT sobre alumbrado de emergencia y el Real Decreto 314/2006, de 17 de marzo, por el que se aprueba el Código Técnico de la Edificación (CTE).

Respecto a la detección de incendios, la norma UNE 23007-14:2014 proporciona las directrices para el despliegue de sistemas automáticos de detección y alarma de incendio dentro de edificios y alrededor de los mismos.



En la Orden INT/316/2011, de 1 de febrero, podemos encontrar las normas que regulan el funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada.



Para saber más

El siguiente enlace te informa sobre la **Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.**

 [Utilización de videocámaras en lugares públicos.](#)

1.4.- Protección de datos y su normativa.



Caso práctico

Valle sabe que cuando se trabaja con datos personales hay que ser muy estricto cumpliendo la Normativa que regula la captación y tratamiento de los mismos porque, en caso contrario, pueden surgir problemas legales.



En la actualidad, son muchos los medios posibles para captar, procesar y almacenar datos personales y esto puede dar pie a un uso fraudulento de los mismos que podrían ocasionar graves perjuicios en la intimidad y privacidad de las personas. Para evitarlo, es necesario que el tratamiento de estos datos, sea cual sea el entorno en el que nos encontremos, se realice de manera adecuada y dentro de unos límites preestablecidos.

El origen de la Normativa que regula el **Derecho a la Protección de Datos** es La Constitución Española en su artículo 18.4, que dice: "La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".



La **Instrucción 1/2006, de 8 de Noviembre, de la Agencia Española de Protección de Datos**, publicada en el BOE el 12 de Diciembre de 2006 referente a la **captación y el tratamiento de imágenes mediante video vigilancia** destaca que los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en la LOPD. Y para ello, deberán colocar en las zonas videovigiladas al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados. El distintivo tiene que ser como el que mostramos en la imagen y tiene que estar situado en un lugar visible y cumplimentado correctamente con los datos de contacto del responsable a quién poder dirigirse. Por otro lado, sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

Las **cámaras y videocámaras instaladas en espacios privados** no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.

Las **imágenes** sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

Por tanto, esta instrucción se debe de cumplir y las **grabaciones** tendrán que inscribirse en la agencia española de protección de datos. Las grabaciones deberán eliminarse en el plazo máximo de un mes y se colocarán los distintivos informativos, identificando el responsable ante quien ejercer los derechos de protección de datos.



Para saber más

En estos enlaces puedes consultar la información sobre la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y normativa relacionada:

 [Ley de protección de datos de carácter personal.](#)

 [Normativa homologación CCTV.](#)

 [Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.](#)

2.- Intrusion.



Caso práctico

Isidro comenta con su compañero que deberían estudiar analizar los sistemas de intrusión de última generación de vigilancia, por ejemplo, sensores como el de la imagen, para evitar quedarse desactualizados ya que los fabricantes están continuamente sacando al mercado modelos nuevos.



La principal finalidad de los **sistemas anti-intrusión** es asegurar que las personas, propiedades, bienes y activos estén protegidos frente a intrusos, es decir, frente a accesos no autorizados. Estos sistemas además del propio, es decir, alertar en caso de intrusión, deben tener un efecto disuasorio en cuanto que el potencial intruso al advertir la presencia de estos desista en su intento de acceso. Estos sistemas pueden integrarse complementando los sistemas existentes de control de acceso al interior de unas instalaciones.

Es fácil entender que un asalto constituye un grave problema que además de los daños en las instalaciones, en los equipamientos o en los bienes, en ocasiones puede dar lugar a secuelas psicológicas en las personas que lo sufren.

Los **sensores de intrusión** detectaran la presencia de personas o animales y nos alertarán para que, ya sea mediante el empleo de cámaras de CCTV o presencialmente, se verifique dicho acceso y se tomen las medidas establecidas en cada caso. De esta manera podremos mantener controlado el acceso a determinadas áreas.

Las **características de un sistema anti-intrusión** variarán dependiendo de las dimensiones físicas del recinto a proteger y del número de zonas de intrusión que se quieran instalar desde las 4 hasta las 520 zonas.



Estos sistemas están compuestos por:

- ✓ Una unidad de control o Central de alarma.
- ✓ Unos elementos detectores (Sensores).
- ✓ Unos elementos de señalización óptica y acústica (Avisadores).
- ✓ Conexión a CRA (central de recepción de alarmas) o marcación de un número de teléfono.
- ✓ Módulos de conexión /desconexión o teclado.



Reflexiona

¿Por qué normalmente es muy fácil detectar la presencia de un sistema anti intrusión en una instalación desde el exterior?

Mostrar retroalimentación

Por el efecto disuasorio que tienen cuando son advertidos por el posible intruso.



Autoevaluación

Los sistemas anti-intrusión permiten identificar a las personas que cometen la infracción:

- Identifican a la persona que comete la infracción.
- Identifican una entrada no autorizada.
- Solo identifican a las personas que miran a los sensores.
- No identifican personas, identifican fuegos.

Incorrecto, no identifican personas.

Correcto, estos sistemas identifican entradas, no personas.

No es correcto. Los sensores no identifican a las personas que no tienen en la base de datos.

Deberías repasar, no es correcto. Para ello están los sistemas contra incendios.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

2.1.- Detección de intrusión.



Caso práctico

Isidro y su compañero analizan los diferentes tipos de detectores que se encuentran actualmente en el mercado para así saber cuál tienen que elegir en cada situación y también como deben realizar la conexión entre ellos y las central.



Los **detectores de intrusión** son elementos que, conectados a la central del sistema de alarmas, son capaces de comprobar las variaciones de una condición de reposo en un lugar específico, como cambios de temperatura, movimiento o nivel de vibraciones y comunicar esa información a la Central de Alarmas.

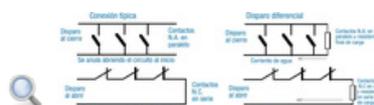
Pueden funcionar con diferentes tecnologías dependiendo del tipo de variaciones que se quieran captar, pero todos tienen en común que producirán variaciones de corriente en las líneas de aviso que los unen con la unidad de control que una vez procesadas darán lugar a la activación de los sistemas de señalización y aviso entre los que encontramos avisadores ópticos, acústicos y llamada telefónicas.

Son de reducido tamaño y, aunque dependiendo del modelo varia, en ningún caso sus dimensiones sobrepasan los 20 cm y su alimentación en baja tensión desde la central suele variar (6 V a 12 Vcc) aunque también los hay sin alimentación, denominados pasivos.

El **sensor en su funcionamiento** provocará la conexión o desconexión de la alarma mediante un interruptor que se abrirá o cerrará dejando de pasar corriente con contactos “**NC**” (normalmente cerrados) o al provocar el paso de corriente en el caso de los contactos “**NA**” (normalmente abiertos). Las líneas balanceadas son iguales, solo que se les ha añadido un resistencia en serie al final de la línea. Cuando hay que instalar varios sensores, éstos se colocan en serie si utilizamos sus contactos cerrados (NC) y en paralelo, si son abiertos (NA). Con el sensor “NC” cerrado la alarma está en reposo y con el sensor abierto la alarma está activa. Pasa al revés con los contactos “NA”.

Cuando conectamos los sensores mediante el sistema de cableado convencional, el “bucle” o circuito cerrado-abierto, además de la línea de circuito de disparo para sus contactos, debe llevar la **línea de alimentación común** a todos los sensores y dos hilos más para el circuito antisabotaje o “**tamper**”, que se activa al intentar manipular o abrir el detector. Serán 6 cables en total salvo que se empleen sistemas **multiplexado** que sólo se necesitan 2 o 3 hilos para todas las funciones.

En algunos casos, se instalan **sensores vía radio**, que son muy parecidos a los anteriores a los que se les ha añadido un pequeño emisor de radio, tienen un alcance limitado y se alimentan con una pila. Cuando las distancias entre el detector y la central son grandes podemos recurrir al empleo de repetidores. Como veremos en posteriores unidades, los sistemas inalámbricos tienen algunas ventajas, pero también algunos inconvenientes como que pueden ser fácilmente saboteados con **inhibidores de frecuencias**.





Autoevaluación

¿Que utilidad tienen las baterías en los sistemas anti-intrusión?:

- Ahorrar energía.
- Para permitir que el sistema funcione cuando falte la corriente alterna.
- Permiten que los sensores estén activos en todo momento.
- Detectar la intrusión.

Deberías repasar. Las baterías no sirven para ahorrar energía.

Muy bien, efectivamente las baterías sirven para proporcionar energía al sistema en caso de fallo energético.

No es correcto. Las baterías suministran corriente continua a todo el sistema.

Incorrecto. La batería no sirve para detectar nada.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

2.2.- Niveles de intrusión.



Caso práctico

Isidro, junto con su compañero, va a identificar los detectores de intrusión que existen en el mercado para poder elegir el más adecuado a cada situación y tienen que tener muy en cuenta como los van a colocar, en serie o en paralelo.



Tal y como hemos comentado anteriormente podemos distinguir **3 niveles de protección**:

- ✓ **Primer nivel de protección, zona periférica.** Se vigila el perímetro de una instalación. Estos sistemas se basarán en la detección infrarroja, los ultrasonidos, la detección magnética y las cámaras de videovigilancia.
- ✓ **Segundo nivel, las zonas de acceso, zonas exteriores.** Se protegen las zonas de acceso, pasillos, ascensores, escaleras, exteriores, habitaciones. Se utilizarán detectores comunes a los colocados en zonas periféricas y de interior.
- ✓ **Un tercer nivel, zona de interior.** El lugar principal que se debe vigilar. Es la zona en la que se encuentra el principal elemento a proteger, cajas fuertes, vitrinas con joyas o similares.

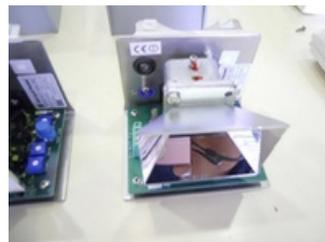
2.3.- Detectores de interior.

Son sensores utilizados para la detección de movimiento dentro de un volumen determinado. Basan su funcionamiento en un interruptor que al cambiar de posición activa una señal de alarma en la central y su alcance es configurable estando limitado a unos **15 metros como máximo**. Se utilizan en interiores de recintos y podemos destacar los siguientes:

1. **Sensor por microondas.** Este detector de tipo radar está compuesto por dos partes: un emisor y un receptor. El emisor emite unas ondas electromagnéticas en la banda X es decir unos 10 Ghz (*1Ghz equivale a 10^9 Hz*), que se reflejan en las paredes del área que estamos protegiendo y vuelven al receptor para ser captadas por una pequeña antena. En condiciones normales, el detector tiene en cuenta la onda reflejada captada por una pequeña antena y queda en situación estable; cuando varía el volumen al entrar un objeto en la zona protegida, varían las frecuencias de las ondas reflejadas y captadas, esa variación de frecuencia activará el detector y por tanto la central de alarma.
-
2. **Sensor por infrarrojos pasivo.** Los rayos infrarrojos son rayos no visibles que se comportan como la luz. Se transmiten como un haz en línea recta y pueden ser reflejados por cualquier superficie brillante. Podemos visualizar una imagen infrarroja debido a que el cuerpo humano emite calor en forma de radiación infrarroja de una longitud de onda proporcional a su temperatura y los detectores de este tipo funcionan captando esta radiación.
 3. **El detector de infrarrojos está basado en un semiconductor llamado foto transistor**, que varía su conductividad con relación a la radiación infrarroja captada por la lente. El detector tiene una especie de óptica que divide la recepción del área en una serie de haces de captación parecida a un abanico cuyo vértice será el propio detector. Utilizan la denominada **lente de Fresnel**.
 4. **Normas a tener en cuenta:**
 - a. Deben estar protegidos de los rayos solares.
 - b. No deben instalarse en exterior.
 - c. No instalar en zonas de temperaturas altas.
 - d. No instalar en pasos de animales.
 - e. No exponerlos a calefacción.
 - f. Instalarse para que los intrusos corten **transversalmente** los haces.
 5. **Sensores microfónicos** que detectan la rotura de vidrio. Están compuestos por un micrófono de alta sensibilidad. Se activan por medio de los sonidos agudos de determinadas frecuencias, siendo inalterables ante sonidos graves. Se utilizan para proteger cristales. Nunca se instalan en la superficie a proteger, se instalan cerca de la misma en paredes y techos. No suelen tener falsas alarmas. Cuando se produce una rotura del cristal se provocan dos tipos de sonidos de distinta frecuencia. El primero es debido al impacto sobre el cristal, un sonido grave de unos 200 Hz; el segundo, debido a la rotura del cristal, un sonido agudo de 3.000 a 5500 Hz. Ambos se tienen que producir en menos de 10 m/seg. El micrófono es sensible a esas frecuencias y a esa secuencia.
-
6. **Detector ultrasónico.** Funciona igual que el de microondas pero con frecuencias de entre 20 y 40 KHz. Esta señal es generada por un pequeño altavoz. Dicha señal rebotará en la pared o en el objeto y será recibida por un micrófono, que convertirá esa frecuencia en señal eléctrica. Un comparador compara la frecuencia de la señal generada con la recibida y si hay diferencia se activará el detector disparando la alarma. Se utilizan para cubrir zonas pequeñas (interiores de vitrinas, coches) y en grandes zonas de 200 m².
 7. **Detectores de doble tecnología.** Basan su funcionamiento en dos tecnologías. Detección por infrarrojos y detección por microondas. Es como si se instalasen dos detectores diferentes y sólo se activan cuando los dos detecten la señal a la vez. Algunos modelos tienen el inconveniente que si se tapan son inútiles, por ello vienen con un sistema de protección llamado antienmascaramiento. En el momento de tapanlos producen una señal de alarma, advirtiendo así de su manipulación y si son manipulados cuando el sistema está desconectado, este dará aviso en el momento de su conexión.

2.4.- Detectores de exterior.

Se emplean para proteger zonas amplias y al exterior y consisten en **sensores lineales** que cubren superficies alargadas y estrechas a lo largo del perímetro. Obviamente tienen que estar preparadas para su instalación en el exterior expuesta a las inclemencias meteorológicas. Los tipos principales son:



1. **Sensores de barrera de infrarrojos.** Estos sensores se pueden instalar tanto en interior como en zonas exteriores. El sistema lo forma un emisor y un receptor de haces de luz invisible que están enfrentados. El receptor se activa cuando son cortados los haces paralelos por un objeto. Para evitar falsas alarmas, el sistema solo se activará cuando se interrumpa más de un haz simultáneamente. Se utilizan para proteger los perímetros.
2. **Sensores de barrera por microondas.** Tienen un emisor y un receptor instalados uno frente al otro. Crean un lóbulo de protección de dimensiones variables en función de las antenas empleadas, de la distancia entre los aparatos y de la sensibilidad ajustada. Cuando el receptor detecta una diferencia de condición dentro de su haz produce una señal de alarma. Según el modelo varía el alcance pudiendo llegar hasta los 700 m. Trabajan en Banda X es decir 10GHz y su alimentación consiste en una tensión continua entre 13,8 Vcc. y 24 Vcc. o en alterna 18 Vcc. Se utilizan para alta seguridad, como protección de las cárceles, centrales eléctricas, refinerías, bases militares, aeropuertos.
3. **Sensores sísmicos de vibración.** Estos sensores se colocan sobre una superficie que al recibir un golpe o una vibración se produce la separación de dos masas que existen en el interior del sensor y esto origina la interrupción del circuito eléctrico. Los hay  piezoeléctricos, de mercurio, péndulo. El piezoeléctrico es extremadamente sensibles y reaccionará si se intenta cortar el cristal, la vibración de este generará un voltaje que activará la señal de alarma. No se debe colocar cerca de paso de coches, camiones o de vibraciones externas. El de mercurio funcionará al moverse la gota de mercurio que unirá eléctricamente dos contactos cerrando el circuito y activando la alarma. Son propensos a falsas alarmas. Están en desuso. Se coloca en cristales y ventanas.
4. **Sensor de cinta autoadhesiva conductora.** Es una cinta adhesiva de material conductor que se adhiere sobre un cristal o superficie a proteger. La cinta es conductora y tiene una resistencia óhmica en función de su longitud. Cuando aplicamos una diferencia de potencial en sus extremos hacemos circular por ella una corriente que se interrumpe al romper el cristal provocando la activación de la alarma. Tiene el inconveniente de que el ladrón la ve y puede cortar el cristal eludiéndola. Hay que colocarla entera, si la cortas puede producir falsas alarmas al variar su resistencia.
5. **Sensor por contacto magnético.** Se emplean para detectar la apertura de puertas, ventanas y persianas. Su funcionamiento se basa en la separación de unas láminas finas que por la acción de las fuerzas del campo magnético formado por un imán cierran un circuito eléctrico. Al abrir la puerta o ventana separa el imán de las láminas y estas abren el circuito eléctrico produciendo la señal de alarma. En la parte móvil de la ventana o puerta se instala el imán y en la parte fija del marco está el sensor. En condiciones normales los contactos están cerrados, formando un circuito en serie.
6. **Vallas sensorizadas.** No son sensores propiamente sino vallas a las que se les han añadido sensores de diferentes tipos como vibración, ópticos, tensión mecánica y que disparan la alarma al mover la valla y separar los contactos interiores del sensor.
7. **Alfombra que detecta las pisadas.** Son sensores ocultos que se colocan debajo de alfombras y que al ser pisadas activan el circuito. Suelen generar una zona de detección volumétrica que se instala siguiendo el relieve del terreno y que es capaz de detectar y localizar el paso de intrusos por el perímetro de una propiedad.



Reflexiona

¿Sabes por qué los sensores de barrera infrarrojas se deben evitar colocarlos en el exterior en zonas abiertas?

Mostrar retroalimentación

Se pueden activar por el paso, por ejemplo, de un animal, creando una falsa alarma.



Autoevaluación

¿Qué tipo de sensor utilizarías para detectar el paso de personas por una zona estrecha y que nadie pudiera ver el sensor?

- Sensor por contacto magnético.
- Alfombra que detecte las pisadas.
- Sensor sísmico de vibración.
- Sensor de infrarrojos de doble luz.

Deberías repasar.

Muy bien, tienes claros los conceptos.

No es correcto.

La respuesta no es correcta.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

3.- Incendio y gases.



Caso práctico

A **Isidro** lo han llamado para que realice una instalación de detección de incendios. Conoce bien estos sistemas y está deseando poner en práctica todos los conocimientos adquiridos durante sus estudios. Para llevar a cabo esta tarea, en la empresa le han dicho que le acompañará un instalador no cualificado.



Empezaremos por aclarar el que se entiende por detección de incendios. Llamamos **detección de incendios** al hecho de detectar y alertar de un incendio en una ubicación perfectamente definida. Ante un incendio, una pronta detección y respuesta es el factor más importante en un sistema de seguridad para evitar un desastre y generar operaciones automáticas para proteger a las personas y a los bienes a través de la instalación de dispositivos, equipos y sistemas electrónicos y/o eléctricos como pueden ser un extractor.

Es importante saber que las **alarmas contra incendios** están continuamente en funcionamiento independientemente de que haya personas o no en el sitio en cuestión, además, es obligatorio su uso en determinados locales de uso público, industriales y garajes. Normalmente esta central está supervisada por personal especializado que actuará según el plan establecido en caso de alarma.

En el caso de **alarmas de detección de gases** dependiendo de las características del gas a detectar instalaremos el detector más apropiado. Sabemos que hay gases más pesados que el aire y otros que son más ligeros, por lo cual tendremos detectores que colocaremos en el techo y otros que pondremos en el suelo o en la zona baja de la pared. También podemos encontrar para las viviendas pequeños detectores independientes con alarma y alimentación incorporadas. Cuando los detectores perciben una concentración superior a la recomendable se activan emitiendo una señal y activando sistemas de extracción de gases.



Existen dos sistemas diferentes de alarmas:

- ✓ **Sistema de detección convencional o de identificación colectiva.** Cuando se dispara una alarma en la centralita solo podemos tener conocimiento de la zona en la que se encuentra el dispositivo que ha sido activado, pero sin saber con exactitud cual ha sido el causante de la misma. En los casos de hoteles, por ejemplo se colocan en el exterior de las puertas unos indicadores para poder localizarlo sin tener que abrir todas las habitaciones.
- ✓ **Sistema de detección microprocesado con identificación individual en sus elementos.** Este sistema permite la identificación individual de cada elemento de detección de manera que en caso de alarma podamos saber exactamente que dispositivo es el que ha sido activado y no solo en que zona se encuentra, tal y como sucede con en los sistemas convencionales.

3.1.- Detección de incendio y gases.



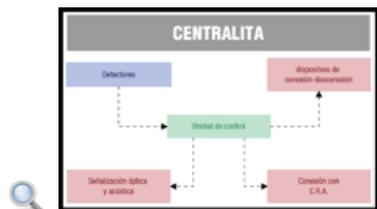
Caso práctico

Isidro conoce muy bien la composición de estos sistemas y le explica al instalador que la instalación debe cumplir con la normativa ya que, en caso de que la instalación no esté bien realizada, seremos nosotros los responsables. Le explica además, la importancia de saber elegir la central más adecuada a cada lugar.



Un **sistema de detección de incendios y gases** estará compuesto de:

- ✓ Una unidad de control que recibe la información de los detectores.



Composición de un sistema de seguridad.

- ✓ Los elementos detectores, que son los encargados de identificar las causas que provocarán la activación de la central, enviando una señal eléctrica a la central para que ésta la procese y actúe en consecuencia.
- ✓ Por otro lado, tenemos los dispositivos de conexión-desconexión con los cuales interconectamos los dispositivos, a través de cables coaxiales, mangueras multicable o con ondas de radio.
- ✓ Los elementos de señalización óptica y acústica, que están controlados por la unidad de control y nos informarán del estado de la central de alarma, comunicándonos si está en reposo o activada. Utilizan elementos de aviso de tipo luminoso o sonoro.
- ✓ Por último, estas están conectadas a la central receptora de alarmas a través de su modulo correspondiente de conexión C.R.A.

Sabemos que estos equipos se deben instalar obligatoriamente en locales de uso público e industriales, así como en garajes, lo que está indicado en las ordenanzas municipales de cada ciudad y que por tanto se debe cumplir.



Citas para pensar

"Fiarse de todo el mundo y no fiarse de nadie son dos vicios: pero en el uno se encuentra más virtud, y en el otro más seguridad."

Séneca, Lucio Anneo.

3.2.- Detectores. Características y tipos.



Caso práctico

Para saber que tipo de detector elegir en cada situación lo mejor es conocer el funcionamiento detallado de cada uno de ellos. Isidro y su compañero buscan en Internet catálogos de fabricantes para estar informado de las últimas tecnologías a la hora de implementarlas.



En los **sistemas de alarmas contra incendio** utilizaremos detectores que nos informen de la presencia de humo, fuego, aumento de temperatura en un pequeño periodo de tiempo y gases. Los detectores pueden ser automáticos o manuales, es decir se necesitará que una persona los accione manualmente en función de como se activen.

El manual se activa por contacto al pulsarlo, ya sea normalmente cerrado "NC" o normalmente abierto "NA". Su funcionamiento es abrir o cerrar un circuito eléctrico que está cableado hasta la central. Una vez que la central detecta la apertura o el cierre de dicho circuito, realizará la activación de la alarma. La conexión de los detectores normalmente cerrados se realizará conectando todos los sensores en serie con la central cerrando el lazo con una resistencia de final de línea. En el caso de los detectores normalmente abiertos deben conectarse en paralelo.

Los **automáticos** basan su funcionamiento en la variación del consumo de  corriente. Este tipo de detectores están consumiendo una corriente eléctrica de un valor muy pequeño, al rededor de los 100 microamperios, cuando están en estado de reposo. Cuando se activan debido a la detección de fuego, humo o gas aumentan su consumo de corriente pasando a alrededor de los 200 miliamperios, aumento que es detectado por la central de incendios o gases que responderá activando el sistema de alarma.

- ✓ Detectores iónicos de humo, Detecta las partículas iónicas en suspensión en el aire que se produce al inicio de un fuego.
- ✓ Detectores térmicos de temperatura fija. Detectan la elevación de temperatura por efecto de las llamas. Se montan donde se prevea una elevación rápida de la temperatura en caso de incendio.
- ✓ Detector Térmico-Termovelocimétrico. Se basan en la detección por temperatura fija, y por  gradiente de temperatura (cuando la temperatura aumenta de forma gradual, suele ser entre 4 °C y 10 °C por minuto.) Se instalan donde se prevean que no se originan humos con líquidos combustibles.
- ✓ Detector de llama. Pueden ser de infrarrojos (IR) y se instalan donde se prevean un inicio con radiación infrarroja de la llama.
- ✓ Detectores de llama ultravioleta (UV), se instalan cuando se prevea que la llama es de radiación ultravioleta, como por ejemplo los gases de combustibles como el butano o el metano.
- ✓ Detectores de (UV + IR) es la unión de los dos anteriores.
- ✓ Detectores de alarmas técnicas. Son detectores específicos utilizados para detectar niveles de líquidos, sondas de humedad, de sustancias químicas y similares.
- ✓ Lineales infrarrojos o barrera de infrarrojos. Se utilizan en detección de humo, en grandes volúmenes y con grandes alturas de más de 14 metros. Tienen un alcance de aproximado de 10 a 100 m.
- ✓ Cable detector lineal de temperatura. Es un cable paralelo en el que se funde la capa aislante y produce un cortocircuito. Se emplea en galerías de cables, colocados en zig-zag sobre las bandejas.
- ✓ Pulsadores de contacto. Se montan en serie junto con el resto de detectores. Es importante saber que cuando transmiten la señal es por haberla activado alguna persona. Esta alarma tiene prioridad sobre la indicada por otro sensor de incendio, ya que actúa antes que el detector las perciba. Estos tienen que

estar visibles. Debemos instalar una resistencia eléctrica de un valor determinado (las hay de 680 ohm, 2k2...) dependiendo del fabricante, para que esta cierre el circuito entre los dos conductores (negativo y línea) provocando la corriente que activará la alarma de incendios.

- ✔ Detector de  monóxido carbono CO. Estos detectores nos avisan de una concentración peligrosa y lo comunican a la central con un cambio de estado. El monóxido de carbono es un gas producido por los motores de combustión y explosión. Al mezclarse el oxígeno con el combustible se produce la combustión dejando libre CO con más gases.
- ✔ Detector Óptico de humo o Fotoeléctrico. Dentro de esta tecnología hay 2 tipos, fotoeléctrico por haz reflejado y de rayos proyectados. Este detector por haz reflejado tiene en su interior una cápsula en la que pueden entrar las partículas de humo. En este recinto hay un emisor de luz y un detector de luz separados por una barrera, cuando en su interior entra el humo la luz es reflejada por las partículas de humo y el detector las capta produciéndose la activación del detector. El emisor de luz normalmente emite destellos que el receptor no recibe y por lo tanto no activará la alarma. Cuando se crea una combustión, las partículas de humo penetrarán en la cápsula y crearán la difracción de la luz del flash, reflejando los destellos hasta la célula fotoeléctrica y variando su resistencia interna, produciendo así una variación de la corriente de reposo que será detectada por la central de alarma.
- ✔ Detector Óptico de llamas. Se basa en el funcionamiento de un detector fotoeléctrico el cual, al recibir las radiaciones infrarrojas o ultravioletas emitidas por las llamas de un incendio, activará la central de alarma.

3.3.- Elementos de señalización acústicos y luminosos.



Caso práctico

Isidro tiene claro que los elementos de señalización son elementos importantes de esta instalación ya que si no señalizamos adecuadamente el inicio del fuego, podemos sufrir sus consecuencias como un retraso en la evacuación.



Los **sistemas de señalización acústicos y luminosos** informan de manera rápida de una alarma a todas las personas presentes en las instalaciones, independientemente del idioma que hablen y entiendan. Estos dispositivos le dan sentido a la instalación de seguridad, ya que de no contar con ellos de nada servirían las alarmas que hayamos instalado para evitar y avisar de robos e incendios. La aplicación de los colores de seguridad se hace directamente sobre los objetos, elementos de máquinas, equipos o dispositivos.

Los **colores** aplicables son los siguientes:

Rojo significa parada, prohibición, incendio, utilizados en pulsadores de alarmas, sistemas ópticos.

Amarillo indican precaución, utilizados en señales de electrocución o conexiones eléctricas.

Verde denota condición segura, excepto en incendio para indicar salidas de emergencia.

Azul indica obligación, en equipos de seguridad.

Los **sistemas acústicos** pueden ser sirenas interiores, sirenas exteriores, campanas, zumbadores, timbres. De todos los sistemas es conveniente montar al menos una sirena exterior aunque el sistema esté conectado a CRA ya que de esta manera utilizamos su efecto disuasorio, con una potencia entre 100 y 130 dB.

La **sirena exterior** estará autoalimentada (con baterías recargables) y autoprotegida mediante tamper, con el fin de evitar manipulaciones. Gracias a la autonomía facilitada por la batería, seguirá funcionando aunque sea arrancada de su emplazamiento. Los elementos acústicos de interior son colocados con el fin de dar aviso a las personas del interior.

Una sirena debe tener un nivel sonoro mínimo de 65 dB o de 5 dB por encima de cualquier otro posible ruido, debiendo adoptarse el valor más elevado de ambos. Si la alarma tiene por objeto despertar a personas que estén durmiendo, el nivel sonoro mínimo deberá ser de 75 dB. Estos niveles sonoros mínimos deberán alcanzarse en todos y cada uno de los puntos en que se requiera escuchar la alarma. El nivel sonoro no deberá exceder de 120 dB en ningún punto situado a más de 1 m del dispositivo de señal acústica.

Los **sistemas ópticos**, pilotos de neón, bombillas o faros rotativos, luces intermitentes, flash estroboscópico, tienen la misión de llamar la atención para ayudar a localizar el lugar donde se ha producido la alarma. El Flash estroboscópico es de 180° de visibilidad. La alimentación suele ser de 24 VCC.

Las **centrales de alarma** (CRA) que funcionan con detectores por zonas indican por medio de un pequeño led, la zona donde se produce la alarma. Actualmente casi todas las centrales tienen una pantalla de LCD en la que nos informan de los eventos ocurridos. Igualmente están protegidas por medio de interruptores tamper, que al tratar de abrirla o arrancarla dan señal de alarma. Estos interruptores están alojados en la tapa

frontal y en la cara que se sujeta con la pared. Normalmente se instalan la sirena y el piloto flash juntos.

Por último, decir que la **iluminación de emergencia**: alumbrado de seguridad (evacuación, anti-pánico, zonas de alto riesgo) y alumbrado de reemplazamiento, se explica en el [REBT](#) en la [ITC-BT28](#).



Autoevaluación

¿Qué detectores detectan antes el fuego, los ópticos de llama o los de humo?

- Los dos al mismo tiempo.
- Indistintamente.
- El de humo antes que el de llama.
- El de llama antes que el de humo.

Deberías repasar.

Muy bien, tienes claros los conceptos.

No es correcto.

La respuesta no es correcta.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

4.- Transmisión.



Caso práctico

Isidro tiene que acompañar al instalador que se ocupa de las telecomunicaciones. Antes de salir de la sede de la empresa hace un listado con los materiales y que herramientas les van a hacer falta para que cuando se encuentren trabajando en empresa cliente tengan a mano todo lo necesario. El instalador amablemente le ha facilitado un listado con todos los materiales que les serán necesarios y las herramientas emplearán.



Un **sistema de señalización a distancia** se utiliza para comunicar una señal de alarma inmediatamente entre la central de alarma de un local con la central de recepción de alarmas.

Los sistemas utilizados pueden ser a través de radio o vía telefónica. Cuando por diversos motivos, como por ejemplo la necesidad de cubrir grandes distancias hace imposible la comunicación vía radio se emplea la telefonía tanto fija como móvil quedando relegada en la actualidad el uso de conexiones vía radio a instalaciones que no pueden disponer de la telefónica.

El tipo de comunicación utilizado con las centrales receptoras suele ser por línea telefónica analógica convencional, apoyado con un sistema de transmisión GSM 3G. La definición técnicamente correcta es UMTS (Servicio Universal de Telecomunicaciones Móviles), LTE para 4G que responde a las siglas Long Term Evolution (evolución a largo plazo) y hace referencia a la tecnología de banda ancha inalámbrica que sirve para la transmisión de datos con la finalidad de dar acceso a Internet a los dispositivos móviles y, por último, ahora la tecnología 5G que es la quinta generación de tecnologías de telefonía móvil y la sucesora de la tecnología 4G. En la actualidad, existe un Plan Nacional de El **Plan Nacional 5G** nace con el objetivo de situar a España entre los países más avanzados en el desarrollo de esta nueva **tecnología**. De este modo, cuando la 5G alcance su madurez tecnológica y comercial, España estará preparada para aprovechar al máximo las oportunidades de este nuevo paradigma tecnológico.

Si el cliente dispone de red  ADSL se instalará además el sistema de transmisión por IP. Hay sitios donde no existen líneas telefónicas analógicas por lo que se instalan sistemas GSM 3G para realizar comunicaciones por IP. Donde no existe cobertura de GSM se instalan sistemas vía satélite.

Su funcionamiento técnico es el siguiente: cuando el analizador detecta un estado de alarma manda una señal al grabador y a la central de proceso. Dicha central da la orden al marcador telefónico, que puede estar integrado en la central, bloqueará el teléfono para que no se pueda recibir llamadas y marca automáticamente, por medio de una señal codificada, estableciendo la comunicación con la CRA. Además, si realizan un sabotaje en la línea de teléfonos, el sistema comunicará la transmisión por línea de telefonía móvil GSM 3G, evitando la incomunicación con la central de alarmas. Así mismo, accionará un relé que conecta a una zona de alarma e informa de la falta de línea. Otro relé, informa sobre algún fallo del sistema, como puede ser la falta de señal en el celular o baja tensión de alimentación. Puede alimentarse desde la batería del sistema de alarmas. Tiene indicadores luminosos sobre el estado del sistema, alimentación y conmutación.

Los requisitos funcionales y de supervisión se detallan en la norma **UNE EN50131-1** y permiten una identificación rápida, así como las acciones a tomar para reducir al mínimo el tiempo de inactividad del sistema.



Debes conocer

¿Sabes qué es VoIP?

VoIP proviene del inglés **Voice Over Internet Protocol**, que significa "Voz sobre un Protocolo de Internet". Básicamente **VoIP** es un método por el cual tomando señales de audio analógicas del tipo de las que se escuchan cuando uno habla por teléfono se las transforma en datos digitales que pueden ser transmitidos a través de internet hacia una dirección IP determinada.

El VoIP permite la unión de dos mundos históricamente separados, el de la transmisión de voz y el de la transmisión de datos. VoIP puede transformar una conexión standard a internet en una plataforma para realizar llamadas gratuitas por internet. Usando algunos de los software gratuitos para llamadas **VoIP** que están disponibles en internet estamos salteándonos a las compañías tradicionales de telefonía, y por consiguiente, sus tarifas.



Para saber más

En este enlace puedes acceder al este interesante pdf en el que tienes más información para que sepas elegir el medio adecuado en la transmisión teniendo en cuenta una serie de parámetros como son: la Velocidad de Transmisión, Atenuación, Características de los dispositivos, equipos a conectar, Inmunidad al ruido.

 [Características y parámetros en los medios de transmisión.](#) (0.67 MB)

4.1.- Medios de transmisión.



Caso práctico

Isidro está analizando que el empleo de cable de cobre para las comunicaciones es una buena opción, pero baraja otras posibilidades así que decide contactar con un comercial de una empresa de materiales para telecomunicaciones.



El **medio de transmisión** es el soporte empleado para la comunicación de las señales con los diferentes elementos de un sistema. Dependen en gran medida de los medios disponibles en el lugar de la instalación. Dependiendo del medio físico utilizado en la transmisión, puede ser: cableado o inalámbrico.

✓ Mediante Cable:

Se utilizan un número determinado de pares de hilos que puede ser de 1 a 4, es decir de 2 a 8 hilos. Para realizar la instalación de interior del abonado con el terminal telefónico se utiliza el cable paralelo bifilar. Este tipo de conductor es de cobre rígido de 0,5 mm de diámetro aunque con la nueva reglamentación de ICT, para distancias inferiores a 100 metros se viene empleando cable de pares trenzados no blindado, UTP.



El cable coaxial. Está formado por dos conductores, uno interno denominado vivo y otro externo, que rodea al primero llamado malla y que sirve de apantallamiento ante interferencias externas. Los dos conductores están separados por un material dieléctrico. El conjunto tiene un aislante externo. Esta configuración permite blindar la señal ante interferencias.

✓ La fibra óptica.

Este otro medio de transmisión empleado en redes para la transmisión de datos consiste en un hilo de pequeño diámetro fabricado con material transparente, normalmente fibra de vidrio o plástico transparente a través del cuál se lanzan pulsos asociados a la información a transmitir. La señal luminosa que transmite en el interior de este hilo, rebotando en sus paredes y avanzando hacia el otro extremo. Una vez montada la infraestructura, el empleo de este sistema permite la transmisión de datos con gran ancho de banda y a grandes distancias. Una de las ventajas es que es inmune a interferencias de tipos magnéticas y eléctricas. Al no ser metálico, no sufre corrosión ni cortocircuito. Las principales desventajas consisten en la fragilidad de la fibra, dificultad a la hora de realizar los empalmes. A pesar de poder realizar las uniones con diversas tecnologías, la más efectiva es la soldadura. Otras desventajas es que no sirven para transmitir energía eléctrica que permitiera la alimentación de repetidores intermedios y no existen memorias ópticas. Las fibras ópticas, según las trayectorias en la propagación del rayo de luz estas pueden ser  multimodo o  monomodo. En los extremos se emplean unos transductores que convierten la energía eléctrica en luminosa y al revés.

✓ Inalámbricos.

Las ondas electromagnéticas que utilizamos en la transmisión están comprendidas entre 3 Khz y 30 Ghz. Se pueden transmitir aplicando a un generador de una antena, la corriente alterna originada. Consta de equipo emisor, receptor y repetidores intermedios. Tienen elevadas prestaciones y alcance. Esta transmisión no necesita cables ni medio de propagación ya que se propaga por el espacio a través de ondas electromagnéticas. Precisa de un Modulador de RF y un Demodulador de RF. Las ondas se

propagan a la velocidad de la luz.



Para saber más

En el siguiente enlace además de la constitución del cable coaxial, tenemos los tipos de cables coaxiales con sus nomenclaturas.

 [El cable coaxial.](#)

4.2.- Características de los conectores.



Caso práctico

Llegados a este punto Isidro tiene claro que tienen que elegir un conector adecuado para la conexión de los diferentes elementos que formen el sistema.



A continuación vamos a ver diferentes tipos de conectores utilizados tanto en la transmisión de señales eléctricas como **ópticas**.

Conectores RJ normalizados: Permiten conectar diferentes dispositivos telefónicos. En función de su tamaño y número de conexiones, los conectores se identifican con un número escrito detrás de las iniciales RJ. Estos son los más extendidos: RJ 9 (de cuatro vías) RJ 11 (de 6 conexiones) y RJ45 (de ocho conexiones).



Conector macho BNC para el cable coaxial: Utilizados en la conexión de cámaras, monitores y antenas en un circuito cerrado de televisión. Los hay también tipo macho y hembra.

Conectores más utilizados en la transmisión para fibra óptica:

- ✓ **FC** (Ferrule Connector) conector de Férula, que se usa en la transmisión de datos y en las telecomunicaciones.
- ✓ **FDDI** (Fiber Data Distribution Interfase), interfase para distribución de datos con fibras. Se usa para redes de fibra óptica.
- ✓ **LC** (Lucent Connector) Conector Lucent MT-Array que se utilizan en transmisiones de alta densidad de datos.
- ✓ **SC** (Subscriber Connector) Conector para el Suscriptor y SC-Dúplex se utilizan para la transmisión de datos.
- ✓ **ST** (Straight Tip), Punta Recta, se usa en redes de edificios y en sistemas de seguridad.



Para saber más

En este enlace tienes información sobre fibra óptica, tipos de conectores, aplicaciones, características, tipos.

 [Fibra óptica.](#)

4.3.- Convertidores de medio.



Caso práctico

Isidro sabe que si eligen la fibra óptica tendrán que utilizar convertidores de medio y eso puede encarecer la instalación. Aunque tienen unas ventajas envidiables como la inmunidad a los campos magnéticos.



Son unos transductores que reciben señales de datos de un medio y los convierten en señales de otro.

Por ejemplo un **transductor** que convierten una señal luminosa, por ejemplo una señal transmitida por fibra óptica, en una señal eléctrica que pueda transmitirse por un medio de cobre. Es decir, convierten un tipo de señal un determinado cable “aparezca” como un cable de distinto tipo sin alterar la naturaleza de la red.

Dispone de dos 📌 interfaces dependientes de los medios. Podemos actualizar una red a fibra óptica sin desprenderse de la infraestructura de cobre. Hay convertidores que permiten convertir las señales eléctricas que corren en cobre a señales que se transmiten en fibra óptica. El estilo del conector depende de la naturaleza de los medios que ha de convertir. Los convertidores de medios son tan simples de instalar como parchear cables y conectores.

Un **convertidor de medios** es usado para extender el cableado Ethernet de cable de cobre 📌 UTP a distancias más allá de los 100 máximos permitidos para UTP convirtiendo las señales de voz/video/datos en señales para cableado de fibra óptica. Un convertidor de medios tiene dos tipos de puertos, uno para el cobre y otro para la fibra (normalmente dúplex, pero a veces simplex).



Para saber más

En el enlace puedes encontrar mucha información sobre distintos tipos de medios de transmisión.

 [Tipos de medios de transmisión y características.](#)

5.- Centrales de recepción de alarma. CRA.



Caso práctico

Isidro le comenta al instalador que tiene un amigo que trabaja en una central de alarma y que le va a enseñar las instalaciones para que puedan observar como trabajan en tiempo real. Podrán ver además equipos de última tecnología.



Las **CRA** son centros destinados a la recepción, verificación y gestión de los sistemas de seguridad (incendio, atraco, robo) ubicados en espacios de alta protección o en dependencias policiales. Se trata de garantizar, mediante la gestión remota de la central, el control total de incidencias y establecer soluciones instantáneas. Así mismo, la central receptora de alarmas tendrá que cumplir con las ordenanzas municipales en este asunto.

La **función principal de la Central Receptora de Alarmas** es la recepción de señales emitidas por los saltos de alarmas de las instalaciones de seguridad. Estas señales pueden llegar hoy por 📡 **RTC**, 📡 **GPRS** o 📡 **ADSL** y comprueban el estado de varios elementos de la instalación de seguridad a través de la línea telefónica fija o GSM (móvil) del emisor, poniéndose en contacto con el cliente para verificar que no se trata de una falsa alarma, pidiéndole que se identifique con una clave. Algunos equipos disponen de servicio de habla y escucha que desde la misma central permite comprobar las situaciones la alarma. Posteriormente se da parte al cuerpo de seguridad, dando aviso de hecho y la hora de llamada queda registrada.

Esta central receptora recibirá la señal de alarma. Mediante códigos diferenciados (**DNIS** identificación de número llamado) puede recibir aviso de robo, incendio, atraco y otros servicios como alertas médicas. Prestan servicio las 24 horas y permiten la conexión/desconexión remota de las alarmas. Por otro lado, disponen de conexión con la Policía Nacional a quienes darán aviso en caso de identificar la señal de alarma como verdadera.



Para saber más

El siguiente enlace puede resultarte muy interesante para conocer como deben ser las instalaciones de las empresas que se dedique a la recepción de alarmas, en su artículo 12. Las características que deben tener así como los sistemas para la recepción y verificación de las señales de alarmas, en el apartado 2 del mencionado artículo.

 [Creación de empresas de seguridad.](#)

Las **centrales receptoras** incorporan cada vez más formas de protocolos de comunicación, como la transmisión vía radio, equipos de comunicación IP, módulos **GPRS** de comunicación inalámbrica. Igualmente los datos son encriptados como medida de seguridad para que nadie pueda verlos. Normalmente las centrales emisoras admiten la conexión a varias líneas telefónicas o la conexión por diferentes medios con la Central receptora de alarmas. En muchos casos, admiten también video y audio bidireccional.

6.- Circuito cerrado de televisión. CCTV.



Caso práctico

A **Isidro** le han pedido información para ver si a la instalación que tenía en mente se le puede añadir un circuito cerrado de televisión. Isidro que está muy metido en estos temas ha comentado que no hay problemas en hacerlo, solo hace falta dinero.



Se denomina **CCTV** a un sistema en el que la emisión de la señal recogida por una cámara se hace de forma privada a uno o más receptores de televisión.

Estos sistemas están formados por una cámara de vídeo, el procesador de vídeo que envía la señal al monitor para visualizar la imagen y la videograbadora para grabar las señales procedentes de las cámaras. Podemos tener pupitres de control para mover las cámaras y utilizar ordenadores como elementos de procesamiento y grabación de señales en sistemas de CCTV. Por último, tenemos los cables coaxiales y conectores “BNC” utilizados para interconectar estos sistemas.



Los CCTV se utilizan tanto en instalaciones privadas como públicas, en entornos domésticos, en la supervisión de personas, en el sector terciario, en el control del funcionamiento de maquinaria industrial y en instalaciones de seguridad y vigilancia.

Con un sistema de vigilancia conseguimos una serie de ventajas como pueden ser: Reducir las personas que vigilan la instalación. Disminuir los riesgos físicos del personal. Poder observar sin ser visto. Disuadir al intruso al sentirse vigilado. Identificar al intruso. Comprobar inmediatamente las causas de la alarma.



Para saber más

En este enlace tienes mucha información de catálogos, sistemas digitales de CCTV, grabación y otros equipos empleados en CCTV.

 [Sistemas digitales de CCTV.](#)

6.1.- Principios básicos de video.



Caso práctico

Isidro está modificando el proyecto para incluir el CCTV. Ha hablado previamente con su cliente para saber con que presupuesto aproximado puede contar. Cree que podrá incluir buenos equipos, con cámaras exteriores y carcasas de calidad para proteger las cámaras.



Como hemos visto, **la señal captada por la cámara y convertida en señal eléctrica**, es enviada al procesador de video. Dicho procesador analizara las señales procedentes de las cámaras instaladas. En él configuraremos la hora del sistema, la conexión IP a internet (si la tiene), la función Quad, que permite dividir la pantalla en cuadrantes para visualizar las señales de los diferentes canales al mismo tiempo, y los conmutadores de señales mediante botones el usuario selecciona la señal a visualizar en los monitores. Tienen conectores para la conexión de videograbadores y algunos lo tienen incorporado. Podemos definir el momento de grabación de cada cámara, así como la reproducción de un día en concreto a una hora determinada. El videograbador grabará la señal en un disco duro interno y también tenemos la posibilidad de volcar la señal grabada en un CD o un DVD dependiendo del sistema. Existen procesadores a los que podemos conectar un pupitre de control para poder manejar las cámaras si éstas fuesen móviles a través de un joystick. Y como, todo el sistema estará conectado con cables coaxiales y conectores BNC para las señales de video.

Según normativa podemos definir tres tipos de instalaciones de CCTV, de los cuales podremos realizar ampliaciones:

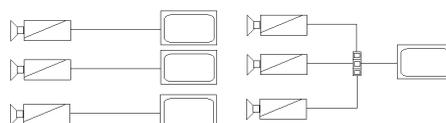
- ✓ Sistema de captación punto a punto.

Es un sistema formado por una cámara y un monitor. La señal obtenida de la cámara es visualizada en el monitor.



- ✓ Captación visual de varias zonas.

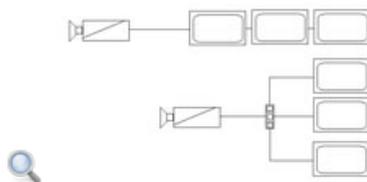
Este sistema está compuesto por varias cámaras enlazadas con su monitor correspondiente o varias cámaras conectadas a un solo monitor, pudiéndose enviar la imagen captada por cualquier cámara al monitor. Visualización simultanea. Es un sistema de visión selectiva.



- ✓ Captación de imagen en puntos concentrados.

En esta situación una sola cámara puede enviar la imagen a varios monitores o seleccionar a que

monitor enviamos la imagen.



Reflexiona

¿Qué utilidad tiene poner 3 monitores a una misma cámara?

Mostrar retroalimentación

Nos da la posibilidad de poderlas visualizar por vigilantes diferentes y ponerlas en diferentes habitaciones.

6.2.- Aplicaciones.



Caso práctico

Isidro le comenta al instalador que una de las aplicaciones de los CCTV es permitirnos visualizar el sistema de imágenes en cualquier lugar del mundo.



Entre las aplicaciones más importantes tenemos:

- ✓ Vigilancia perimetral de todo tipo de instalaciones.
- ✓ Supervisión de espacio de control de acceso y seguimiento de interiores.
- ✓ Control de zonas restringidas.
- ✓ Protección puntual de objetos valiosos.
- ✓ Detección mediante video-sensor.
- ✓ Supervisión de instalaciones a distancia.
- ✓ Grabación, transmisión y almacenamiento de imágenes y sonido.

Como puedes ver la gama de aplicaciones es amplia ya que son muchas y muy variadas. Para hacer más versátiles a estos equipos se les incorporan nuevas funcionalidades pudiendo así emplearse en todo tipo de entornos industriales, en oficinas y viviendas.

6.3.- Equipos: cámaras procesadores, grabadores y monitores.



Caso práctico

Isidro le comenta al instalador que las aplicaciones de los CCTV son tantas como imaginación tengamos para montar un sistema en un lugar determinado del mundo.



La **cámara** es el elemento que capta la señal de vídeo en el sistema. Su misión consiste en convertir las variaciones de luminosidad de la imagen en variaciones de corriente eléctrica por medio de un chip. La cámara está formada por el cuerpo y la lente.

En el **cuerpo** tenemos la electrónica de captación y procesamiento de la señal de vídeo, así como los conectores para la red eléctrica y el conector BNC con cable coaxial para la distribución de video o RJ para cable UTP según sea el caso.

La **lente** es el elemento encargado de enfocar la imagen sobre el CCD, para captar las señales.

Tipos de cámaras. Podemos encontrar una gran variedad de cámaras que se adaptan a los diferentes requerimientos de cada tipo de instalación del CCTV. Estas pueden captar imágenes en color o en blanco y negro.

- ✓ **Cámaras fijas.** Son cámaras que vigilan un punto concreto. No tienen movimiento motorizado y se instalan fijas sobre soportes en paredes y techos. Las que se instalan en el exterior, necesitan de una carcasa de protección de las condiciones ambientales.
- ✓ **Cámaras motorizadas.** Son cámaras fijas que se instalan en un soporte motorizado que permite el cambio de posicionamiento desde una unidad de control.
- ✓ **Cámaras de infrarrojos.** Estas cámaras permiten la grabación de imágenes por la noche con poca luz. Normalmente la cámara dispone de un conjunto de diodos de alta luminosidad que emiten luz infrarroja y permiten la visión en alta oscuridad. Los focos de infrarrojos se instalan al lado de la cámara para facilitar la visión nocturna.
- ✓ **Cámaras domo.** Son cámaras de reducido tamaño para instalación en interior. Disponen de una carcasa de protección semiesférica y una base para fijar sobre techos o paredes. Algunas son móviles mediante un motor y necesitan una unidad de control.

Procesadores. El procesador se utiliza en instalaciones importantes de CCTV. Como sabemos se encarga de recibir todas las señales de las cámaras y enviarlas al monitor, al grabador, a internet o al lugar donde lo hemos configurado.

Grabadores. Los grabadores de video tienen la finalidad de tener un almacén de las imágenes captadas por las cámaras para poder analizar un intervalo de tiempo grabado. Los hay de diferentes tipos. En función del tipo de memoria utilizada pueden ser de cinta, conocidos como VCR, de disco duro DVD, de CD, de memoria Flash.

Un **grabador de vídeo digital** es un dispositivo que se compone básicamente de un disco duro de gran capacidad, un microprocesador y los buses de comunicación; y por otra parte del software que proporciona diversas funcionalidades para el tratamiento de las secuencias de vídeo recibidas, acceso a guías de programación y búsqueda avanzada de contenidos, programación de los tiempos de grabación: intervalos, diarias, semanales, mensuales, así como la selección de los parámetros de activación y desactivación

vinculados a dispositivos de detectores.



Monitores. Son los equipos que muestran las imágenes captadas por una cámara o reproducidas por un grabador. El monitor convierte las señales eléctricas que le llegan en imágenes visibles en la pantalla. Todos ellos deben proporcionar imágenes nítidas y claras. Estos pueden ser monocromo o color. Algunos tienen funciones integradas de cuadrantes, secuenciadores, congeladores de imágenes.



Para saber más

En este enlace tienes mucha información de catálogos de cámaras IP.

 [Cámaras IP.](#)

Anexo.- Licencias de recursos.

Ningún recurso de fuentes externas que requiera citar explícitamente sus datos de licencia ha sido usado en esta unidad, por lo que este anexo queda vacío. Todos los recursos utilizados, de fuentes internas, se acogen al Aviso Legal de la plataforma.