ELEMENTOS TÉCNICOS DE PROTECCIÓN Y SEGURIDAD

S.I.P.L.G.
ÁREA DE PUBLICACIONES

Autor/es: JUAN JESÚS SÁNCHEZ BECERRA
JORGE IGNACIO BORRALLO RIEGO

AUTORES Y EDICIÓN:

© JUAN JESÚS SÁNCHEZ BECERRA

© JORGE IGNACIO BORRALLO RIEGO

Policías Locales de Ronda (Málaga)

COLABORA Y DISTRIBUYE

S.I.P.L.G.
ÁREA DE PUBLICACIONES

EJEMPLAR DE DISTRIBUCIÓN GRATUITA

Esta publicación electrónica se divulga y distribuye con la colaboración de USPLBE, Unión Sindical de Policía Local y Bomberos de España, con la intención de reciclar y perfeccionar en esta materia a los diferentes Policías Locales tanto de nuestra Comunidad Autónoma, así como del resto de Comunidades. Se publica electrónicamente como publicación electrónica en la página web www.escuelapolicia.com, en la sección biblioteca virtual, apartado publicaciones de Interés Policial, estando disponible pasa su visualización e impresión de cuantos usuarios estén interesados en sus contenidos.

INDICE

EPÍLOGO:

Acudimos a nuestro puesto de trabajo a diario, si bien es cierto, no siempre lo desempeñamos en la misma instalación, todo dependerá del servicio que se te asigne, puede ser ofreciendo seguridad en el Ayuntamiento, en una dependencia municipal, pero a diario debemos de pasar las novedades y listas en la Jefatura.

Con esta publicación los autores pretenden ofrecer el punto de vista desde la seguridad que no solo nosotros podemos ofrecer a una instalación, si no la que ella nos puede asegurar a nosotros.

No podemos caer en el error de llegar a pensar ni un solo segundo que por portar un arma de fuego, nadie se atreve a asaltar una dependencia policial, e intentar acometer contra nosotros, nuestra integridad física e incluso contra nuestra vida, cabe señalar solo lo que le pasó no hace tanto tiempo y que empieza a caer en el olvido, al compañero de Puerto Serrano, Juan Cadenas, con el que los autores de esta publicación tuvieron la suerte de compartir Academia.

Toda la seguridad que podamos ofrecer y ofrecernos es poca.

1.- INTRODUCCIÓN.

Se dice que algo es seguro cuando se considera libre y exento de todo peligro, daño o riesgo. consecuente con esta premisa, las personas suelen adoptar toda una serie de precauciones y medidas que garanticen su seguridad, tanto a nivel individual como colectivo.

Si atendemos a estos conceptos podemos definir la seguridad como:

"La protección de personas y bienes por medios humanos y físicos"

"Conjunto de medios humanos, equipos e instalaciones dirigidos a la prevención de riesgos, protección de personas y bienes, buscando minimizar los posibles daños".

Los conceptos y definiciones citadas suelen dar origen a la siguiente pregunta:

¿Por qué la seguridad tiene carácter público y no privado?

Si atendemos a la evolución histórica veremos qué, en un principio, cuando la sociedad se va perfeccionando, surge la necesidad de la seguridad colectiva y se crean los reductos en cuyo interior se protegen los miembros de la comunidad, tanto de las posibles agresiones de animales como de otras tribus.

Con la aparición de grandes núcleos urbanos surge la necesidad de la seguridad "privada", entendido en su concepto más primigenio, como serían las guardias personales, escoltas, etcétera. La evolución de nuestra sociedad, el surgimiento de empresas y la aparición de nuevas tecnologías dan origen a la creación de empresas dedicadas a la protección e investigación privadas y la consiguiente regulación legislativa de las mismas.

Actualmente dicotomía Seguridad Pública o privada. la seguridad es una competencia exclusiva del Estado, lo que no es obstáculo para que, con carácter complementario y subordinado, se admita la concurrencia de una seguridad privada.

La Constitución española de 1978 asumió el concepto de seguridad ciudadana (artículo 104.1), así como el de Seguridad Pública (artículo 149.1.29.ª). Posteriormente, la dos tiene la jurisprudencia han venido interpretando, con matices, estos dos conceptos como sinónimos, entendiendo por tales la actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad ciudadana.

Es a la luz de estas consideraciones cómo se deben interpretar las ideas de seguridad ciudadana y los conceptos afines a la misma, huyendo de definiciones genéricas que justifiquen una intervención expansiva sobre los ciudadanos en virtud de peligros indefinidos, y evitando una discrecionalidad administrativa y una potestad sancionadora genéricas.

Para garantizar la seguridad ciudadana, que es una de las prioridades de la acción de los poderes públicos, el modelo de Estado de Derecho instaurado por la Constitución dispone de tres mecanismos: un ordenamiento jurídico adecuado para dar respuesta a los diversos fenómenos ilícitos, un Poder Judicial que asegure su aplicación, y unas Fuerzas y Cuerpos de Seguridad eficaces en la prevención y persecución de las infracciones.

En el marco del artículo 149.1.29.ª de la Constitución y siguiendo las orientaciones de la doctrina constitucional, la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, tiene por objeto la protección de personas y bienes y el mantenimiento de la tranquilidad ciudadana, e incluye un concepto plural y diversificado de actuaciones, de distinta naturaleza y contenido, orientadas a una misma finalidad tuitiva del bien jurídico protegido. una parte significativa de su contenido se refiere a la regulación de las intervenciones de la policía de seguridad, funciones propias de las fuerzas y cuerpos de seguridad, aunque con ello nos agota el ámbito material de lo que hay que entender por Seguridad Pública, en el que se incluyen otras materias, entre las que la ley aborda las obligaciones de registro documental o de adopción de medidas de seguridad por las personas físicas o jurídicas que realicen actividades relevantes para la seguridad ciudadana, o el control administrativo sobre armas y explosivos, entre otras.

Para complementar lo anterior y ratificar que la seguridad, especialmente de su aspecto de prevención, es un objetivo esencial que abarca tanto al ámbito público como al privado, se promulga la Ley 5/2014, de 4 de abril, de Seguridad Privada, que deja bien sentado el carácter subordinado que tiene la seguridad privada con respecto a la pública, especialmente cuando se trata de posibles medidas de seguridad.

Por consiguiente, la Seguridad Pública es un servicio que se presta por las fuerzas y cuerpos de seguridad, cuyas funciones se encuentran reguladas en la Ley Orgánica 2/86, de 13 de marzo, que en España se concretan en los siguientes cuerpos:

- Cuerpo Nacional de Policía
- Guardia Civil

- Policías Autónomas
- Policías Locales

Tienen ámbito de actuación de carácter estatal el cuerpo nacional de policía y la Guardia Civil, en tanto que las Policías Autonómicas y Locales limitan sus actuaciones a sus respectivos territorios.

1.1.- OBJETIVOS DEL SISTEMA DE SEGURIDAD.

Para que resulte efectivo un sistema de seguridad alcanzar determinados objetivos, tales como:

a) Disuadir: objetivo evidentemente preventivo y que se cumple con la instalación de una eficiente iluminación, barreras físicas, vigilantes…
b) Demorar: función que tiene como objetivo el obstaculizar dificultados de tardar la agresión.
c) Detectar y Alertar: captar el tipo de acción no autorizada, de forma que alerta al resto de compañeros.
d) Identificar: reconocer el tipo de acción no autorizada de forma rápida y fiable.
e) Canalizar: función que nos permite dirigir, indirectamente, a las personas por las vías deseadas, para ejercer un mejor control de la situación.
f) Reaccionar: función generalmente realizada por medios humanos y que tiene como objetivo el poner en marcha las acciones de respuesta, para la corrección de los incidentes y recuperar la normalidad perdida.

1.2.- ESTÍLOS DE UN SISTEMA DE SEGURIDAD.

En un sistema de seguridad se pueden apreciar 3 estilos que se complementan adecuadamente entre sí:

- **Estilo enmascarado**. en el que un gran número de medidas de seguridad quedan ocultas, bien para garantizar su inviolabilidad o bien para tratar de no dar a conocer el valor de los bienes protegidos.
- **Estilo abierto.** también se le denomina estilo visto. defectos eminentemente disuasorios, en el que se parte de la base que el intruso ignora el valor real de los bienes que custodia pero la perfección la utilización de personal uniformado.
- **Estilo mixto.** suele ser más utilizado y con el que se consigue un muy aceptable nivel de distracción y protección está compuesto por una mezcla de estilo cerrado y abierto.

1.3.- EFICACIA DEL SISTEMA DE SEGURIDAD.

Generalmente se suele contratar a la eficacia de un sistema contrastando dos conceptos:

Tiempo de demora. también llamado de retardo y es el que transcurre desde la activación de una alarma hasta que el intruso alcanzó su objetivo.

Tiempo de respuesta. se trata del espacio de tiempo del que se dispone desde el momento en el que se detecta la intrusión, hasta que se logra su interceptación.

1.4.- LA INSEGURIDAD.

Si aceptamos que la seguridad total no existe, también hemos de aceptar que en nuestra sociedad, a veces, la violencia se impone como una forma normal de las relaciones humanas.

La sensación de inseguridad puede llevar a una persona a pensar que puede ser la próxima víctima de un acto delictivo. Tal sensación puede tener su origen en dos factores:

- Un temor concreto, que se produce lógicamente cuando una actividad delictiva se repite con cierta frecuencia en su entorno. se le conoce como inseguridad objetivo real, sensación objetiva, ya que las condiciones en que se encuentre la persona lo hace proclive a ser víctima del delito.
- Un temor difuso, inconcreto, ante circunstancias poco definidas, qué sería la inseguridad subjetiva o virtual, sensación comprensible en una persona, pero que no se atiene a causas razonables de inseguridad.

2.- ELEMENTOS TÉCNICOS DE PROTECCIÓN Y SEGURIDAD. ELEMENTOS PASIVOS.

2.1.- ELEMENTOS TÉCNICOS DE PROTECCIÓN.

En relación con esta cuestión y con carácter previo a su tratamiento, se considera adecuado recordar algunas definiciones al respecto:

- Medidas de seguridad: la disposición adoptada para el cumplimiento de los fines de prevención o protección pretendidos.
- Elemento, producto o servicio homologado: aquel que reúne las especificaciones técnicas o criterios que recoge una normativa técnica al efecto.

- Elemento, producto o servicio acreditado, certificado o verificado: aquel que lo ha sido por una entidad independiente, constituida a tal fin y reconocida por cualquier Estado miembro de la Unión Europea.

2.1.1.- Elementos Pasivos.

Incluidos en el propio plan de seguridad, los elementos pasivos de protección son todos aquellos que, adosados o no al edificio o inmueble, se emplea con funciones de seguridad y con el fin de impedir, obstaculizar o canalizar la penetración de personas en un recinto cerrado.

Estos elementos van a estar ubicados en los diferentes círculos de protección que componen el sistema de seguridad de acuerdo con el nivel de seguridad que se establezca.

Los niveles de seguridad se establecen en función de:

- Las características del edificio.
- Los accesos con que cuenta.
- Número de visitantes.
- Otras circunstancias de interés para la seguridad.

Del volumen eficacia de la conjunción de los medios empleados en un sistema de seguridad podremos deducir si estamos ante niveles de:

- Seguridad Media.
- Alta Seguridad.
- Máxima Seguridad.

En cuanto a las áreas de seguridad hay que decir que dentro del recinto inmueble se establecerán estas en razón de las personas o cosas que allí se ubiquen, de forma que una requerida mayor atención, otras serán de tipo restringido al público, otras de máxima seguridad…

2.2.- LA SEGURIDAD FÍSICA.

La seguridad física es la seguridad formada por esos elementos de carácter estático y permanente que hemos denominado pasivos. Obras de albañilería, madera, metal, vidrio… que formen la seguridad física de un edificio.

Sus elementos suelen ser de carácter permanente una vez instalados en el lugar de destino, ya que la calidad y la forma de llevarse a cabo la construcción es en ocasiones la que va a definir su duración y los resultados en cuanto a la eficacia del servicio.

los situados en el primer círculo de seguridad o círculo más externo están constituidos de materiales de:

- ✓ Mampostería: cerramientos realizados por materiales de albañilería.
- ✓ Métalica: cerramientos por medio cercas de alambre acodadas en la parte superior.
- ✓ Mixtas: compuesta de mampostería y cerca metálica.

Tanto unos como otros delimitan la propiedad o parte más externa del elemento protegido, debiendo tener una altura mínima de 3 metros y si permiten la visibilidad desde el exterior, deberán colocarse seto a plantas ornamentales para impedir o dificultar la visión del interior.

Los materiales empleados en el círculo más interno o tercer círculo, zona que delimita la intimidad o zona destruida del cliente o moradores del inmueble, suelen ser: puertas blindadas, enrejados especiales, acristalamientos blindados…

Como hemos comprobado existe una relación de los materiales a emplear y las áreas, niveles o círculos de seguridad en que nos encontraremos, para adecuarlo identificar los diferentes sistemas o cierre perimetral.

2.3.- SISTEMA DE CIERRE PERIMETRAL.

El cierre perimetral está compuesto por todos aquellos elementos de seguridad física instalados alrededor del inmueble a proteger con la finalidad de conseguir la seguridad del mismo.

2.3.1.- Muros.

Es el sistema más comúnmente utilizado de protección y está constituido de hormigón, piedra u otros materiales de gran resistencia a cualquier ataque externo como puede ser el realizado por medio de proyectiles, explosivos, etcétera. de los medios empleados en los cierres perimetrales este es sin duda el que ofrece mayor garantía de seguridad y de los que supone mayor disuasión a la delincuencia.

tiene además la finalidad, añadida a la seguridad, de delimitar una propiedad. En muchas ocasiones delimita un recinto área peligrosa por contar en su interior material explosivo o con riesgo de incendio.

2.3.2.- Vallas.

Otro tipo de cerramiento perimetral bastante utilizado, y que también suponen una fuerte oposición a la entrada de intrusos y normalmente la disuasión de éstos. el material empleado en su construcción suele ser diverso: enrejados metálicos, telas metálicas, madera.… su finalidad, al igual que en el caso de los muros, impedir la entrada de intrusos y delimitar propiedades o áreas peligrosas.

Los vallados y enrejados son elementos de protección de tipo perimetral que se usan sin necesidad de unas condiciones de seguridad, empleados como cerramientos para la protección contra la intrusión.

2.3.3.- Barrera de detención de vehículos.

Son dispositivos de protección pasiva que mediante barras o hileras de elementos punzantes que, instalados en los accesos se disponen para la detención de vehículos ante la intrusión no autorizada, siendo este elemento de importante aplicación en seguridad privada.

2.3.4.- Alambradas y concertinas.

Dentro de este grupo están los rollos dentados, rollos de alambre de espino, la línea de alambre de espino. los materiales de construcción de este tipo de alambradas y concertinas son el acero cincado, acero tratado térmicamente y acero inoxidable.

2.3.5.- Concertina.

Una concertina un alambre de acero con púas de alta resistencia, amarrado a intervalos para conformar un cilindro. Es una protección que se instala sobre vallas, mallas o muros para dificultar la intrusión.

2.3.6.- Cabinas y mostradores blindados.

Son recintos de seguridad cerrada construidos con mamparas o paneles transparentes u opacos para evitar una agresión exterior.

2.3.7.- Puertas blindadas.

Las puertas de seguridad podemos dividirla en dos tipos: blindadas y acorazadas.

Las blindadas están construidas de chapa de acero y madera que presentan un alto grado de seguridad definido en la norma UNE 108-122. su marco suele estar construido de madera tratada para una mayor resistencia que los modelos estándar. se exige de manera reglamentaria en establecimientos como joyerías, galerías de arte similares, siendo muy común su uso en viviendas privadas.

Las acorazadas están especialmente diseñadas para su instalación en cámaras acorazadas o recintos de custodia de objetos de alto valor. se construyen de chapa de acero especial y rellenas de 1 enemigo de alta resistencia a la fractura. en la construcción del marco suele emplearse el mismo material acerado que se utiliza para la puerta.

2.3.8.- Cristales blindados.

Son los exigidos reglamentariamente a los cerramientos de los recintos de cajas en entidades bancarias escaparate esos lugares de los establecimientos donde se pongan objetos preciosos cuya valor en con su conjunto sea superior a 90000€y en las ventanas huecos que existen en estos establecimientos.

Existen dos tipos: resistentes al golpe y resistentes al disparo

Los primeros son instalados para impedir el ataque personal cuerpo a cuerpo.

La característica principal de los segundos es que pueden recibir impactos de bala disparada por un arma portátil ligera sin que proyecte esquirlas de la cara posterior del blindaje.

Existen diversos niveles de resistencia a la penetración del proyectil según el calibre y la potencia del arma empleada. por ello se utiliza un cristal blindado costilla entre el nivel correspondiente al calibre de 9 mm parabellum, hasta determinado por el calibre del arma larga de guerra, pasando por diversos calibres intermedios

Otra protección consiste en la colocación en la parte interior de los cristales convencionales de una lámina de plástico que impida la visión del interior de las habitaciones, sin que reste la luminosidad necesaria. esto impide que el agresor pueda localizar visualmente movimientos de personas en el interior de los edificios. pueden ser transparentes o traslúcidos y su composición puede ser de una sola lámina, varias láminas y con cámara de aire.

2.3.9.- Esclusas.

Este elemento de seguridad pasiva permite el paso a personas al interior de acuerdo con una información recibida de detector de metales. es de poca utilidad en lugares muy frecuentados por el público.

Se trata de una cabina con dos puertas que conectada a un arco detector de metales, permite el paso en caso de que el detector lo considere procedente. consiste en un

dispositivo que abre una puerta permitiendo el paso a zona o descansillos donde la persona debe esperar a que una segunda puerta le permita el paso definitivo.

3.- FIABILIDAD Y VULNERABILIDAD AL SABOTAJE Y MANIPULACIÓN.

La función de estos medios de seguridad pasivos es que disuadan a la mayoría de los delincuentes o al menos impidan la entrada libremente en un evento cerrado teniendo que emplear otros medios para vencerlos.

Los muros presentan la ventaja de limitar la capacidad de conocer lo que existe tras él pero en cambio permite la escalamiento con gran facilidad sobre todo si se empleará escalera o útil adecuado, dado que la altura de este elemento pasivo no suele ser muy elevada (una media de 3 metros).

Las vallas son, por el contrario, menos resistentes y presentan mayor dificultad para su escalamiento pero en cambio son más vulnerables a la hora de vencer sus resistencias y su eliminación, sobre todo de aquellas construidas delambre que pueden ser perforadas fácilmente con unos alicates.

Tanto las vallas como los muros pueden ser atacadas de forma contundente con la utilización de explosivos, con vehículos potentes como tractores o similares, sorteados a través de zanjas o túneles incluso en plan de la red de tuberías de desagüe del subsuelo de las ciudades. Por otro lado presentan la ventaja de ser completadas con vegetación que limitan la capacidad de conocer lo que existe tras ellos, pero tiene la desventaja en algunos casos de facilitar el escalamiento por la facilidad que presenta a la colocación de utensilios para escalar mejor.

Todos los elementos pasivos de seguridad actúan en principio y su acción al intruso pero eficacia es relativa y depende más de la persona que tenga encomendada la seguridad del elemento a proteger queda fiabilidad del propio elemento pasivo.

Pasando al terreno de los resultados en este campo, solo hay que ver las estadísticas para comprobar el descenso que se ha producido en los atracos a entidades bancarias desde que se procedió a la instalación de medios pasivos de seguridad en sus distintas variantes, como es el caso de la protección de los recintos de cajas con cristales blindados.

3.1.- LUGARES DE INSTALACIÓN DE LOS DISTINTOS MEDIOS FÍSICOS.

Muros y alambradas en zonas perimetrales de los objetos de protección.

Puertas blindadas, acorazadas y esclusas, en el acceso al interior de edificios o locales objeto de protección o en el interior de los mismos.

Cristales blindados, mostradores, cabinas… suelen ubicarse en el interior del edificio o local donde interesa establecer una máxima seguridad por objetos o valores allí depositados.

4.- ELEMENTOS TÉCNICOS DE PROTECCIÓN Y SEGURIDAD. ELEMENTOS ACTIVOS.

4.1.- ELEMENTOS TÉCNICOS DE PROTECCIÓN.

Para adentrarnos en el conjunto de elementos activos en el campo de los medios técnicos de protección, hay que decir dos cosas. por un lado que este tema es complementario del tema anterior donde tratamos los medios de protección de tipo pasivo, que van a ser complementados con otros elementos de tipo activo. por otro que, en la práctica, los medios de tipo pasivo y activos, a la hora de planificar y llevar a un buen término un dispositivo de seguridad, realizan funciones complementarias de forma que no es posible desdeñar a ninguno de ellos si se quiere conseguir la efectividad del servicio.

por elementos de tipo activo podemos entender aquellos que requieren o presentan una actividad dinamismo constante su funcionamiento, no como en el caso de los elementos pasivos que eran de tipo estático y que tras un sabotaje, al no estar conectados con medio activo alguno, no pueden dar respuesta de detección y transmisión necesaria.

Con lo cual tendremos que son elementos que con su presencia van a buscar medidas de carácter actitudinal y que, en Unión de los medios pasivos y humano, tratan de reducir al máximo el factor de probabilidad del riesgo estimado de un determinado lugar. exigen ser controlados por el hombre sin el cual la información sobre seguridad que estos medios proporcionan no tendría eficacia alguna.

4.2.- LA SEGURIDAD ELECTRÓNICA.

En el punto tercero hablamos de la seguridad física y de sus vulnerabilidades, pero la electrónica tiene mucho que decir en la seguridad y podemos afirmar que, dada la fiabilidad

de los sistemas de medios técnicos de protección de tipo electrónico, actualmente son empleados por todas las instituciones o empresas que en el mundo se dedican a la seguridad.

los medios electrónicos de seguridad que se emplean en la protección podemos dividirlos en tres grandes bloques:

- Detectores.
- Centralitas de alarmas.
- Circuito Cerrado de Televisión (CCTV).

4.2.1.- Detectores.

Básicamente es un dispositivo electrónico que produce una señal eléctrica en función de la operación de una magnitud de temperatura, luz, presión, ruido, calor…

El detector funciona conectado a una centralita de alarma, activando en algunos casos sistemas de respuesta como sirenas, cámaras de video, etcétera, que permiten detectar al intruso.

En función del lugar de colocación los detectores podemos dividirlos en: Exteriores e interiores.

Los Exteriores son colocados en la zona perimetral del edificio elemento a proteger permitiendo avisar al centro de control decisorio de la penetración de un intruso.

Los interiores se instalan en aquellas zonas del edificio que requieren una mayor protección o zona de seguridad no se necesita conseguir un tipo de protección integral para qué, mediante su activación, se puede impedir la penetración de un intruso y conseguir su detección, detectar cualquier tipo de incidente, neutralizarlo…

En función del tipo de magnitud los detectores los podemos dividir en:

- Temperatura.
- Ópticos.
- Presión.
- Movimiento,
- Acústicos.
- Vibración y rotura.
- Volumétrico.

En función de la técnica empleada:

- De Técnica infrarrojas.
- De microondas.
- De tensión.
- De presión diferencial.
- De efecto inercial.

Veamos primero los empleados en el interior de inmuebles:

a) De Presión.

Funciona accionando un interruptor o elemento hidráulico cuando se realiza una presión sobre ellos y bajo un determinado peso o ausencia de ellos. Pueden ser electromecánicos o diferenciales y se usan en el suelo en forma de almohadilla o alfombra, en muros y techos.

b) Detectores/Sensores.

Detectores – Sensores de doble tecnología, con el objeto de conseguir la máxima seguridad frente a falsas alarma, se combinan 2 tecnologias distintas, infrarrojos pasivos (detectan los cambios de temperatura que el intruso pueda ocasionar en el medio) y microondas (detectan el movimiento de cueros en el medio). Para realizar el disparo deberán activarse ambas tecnologías. De esta forma conseguimos un detector de muy alta fiabilidad.

c) De vibración.

Se fundamenta en un micrófono o dispositivo similar que registra las vibraciones que se producen en su entorno, aunque frecuentemente se ven afectados por vibraciones externas al lugar de protección. Suelen ser de varios tipos como: los geófonos, inerciales, piezoeléctricos…

Estos instrumentos están diseñados para detectar los pequeños incrementos de desplazamiento lineal que tienen lugar cuando las estructuras o los materiales vibran. Estos instrumentos son útiles en una amplia variedad de aplicaciones como equipos de protección de algunos elementos como cajas fuertes, cámaras acorazadas inspección y procesado de microelectrónica, análisis de componentes y materiales y diseño de máquinas.

d) De tensión.

Su funcionamiento esta basado en la tensión de un hilo metálico que activa la alarma al variar la tensión que posee.

e) Electromagnéticos.

Captan las señales producidas por el movimiento del cuerpo humano cuando éste rompe la emisión de microondas entre un emisor y un receptor lo que produce el disparo de la alarma. Son de gran utilidad por su penetrabilidad a través de la mayoría de los materiales usados en construcción. Puede estar formando barreras de microondas, capacitivos, acoplamiento de conductores o acoplamiento de guias de ondas.

f) Magnéticos.

Se activa la alarma por el desplazamiento de un contacto electrónico sobre un imán permanente y es difícil que se produzca una falsa alarma.

4.2.2.- Radares.

Cuyo funcionamiento es similar a un equipo radar. Emite ondas muy pequeñas las cuales al ser recibidas de nuevo por el receptor indica que han sido absorbidas por algún intruso, activándose de esa forma. Su complejidad provoca que el resultado no sea optimo por el numero de falsas alarmas que produce.

a) De infrarrojos.

Vivimos en un mundo de energía invisible – energía en forma de radiación electromagnética. Hoy, el espectro de la radiación electromagnética es conocido y consiste en un tremendo rango de frecuencias de radiación que se extienden desde los 10 Hz hasta más de 10,20Hz.

Las seis mayores regiones del espectro electromagnético son identificadas por la longitud de onda y frecuencias. Esas regiones incluyen las ondas de radio, las infrarrojas (IR), la luz visible, la ultravioleta, los rayos X y los rayos gamma en orden decreciente de longitud de onda o en incremento de frecuencias.

En el detector de rayos infrarrojos se activa la alarma cuando un rayo de luz infrarroja es interrumpido en su camino entre el emisor y el receptor por un intruso.

Las barreras de infrarrojos de doble Haz, pueden tener dependiendo de la distancia a cubrir, entre 25 a 150 metros.

b) De presión subterránea.

El peso del individuo sobre dos plataformas subterráneas provoca un cambio de la presión que se traduce en una señal eléctrica que activa la alarma.

c) Detectores Infrarrojos Pasivos (PIR).

Un típico ejemplo de energía infrarroja cercana es el control remoto de la televisión. La energía infrarroja que esta muy por debajo de la visible es llamada infrarroja-lejana. Una de las mejores fuentes de energía infrarroja-lejana la que permite a los fabricantes de sensores de seguridad, producir detectores Infrarrojos Pasivo que pueden finalmente detectar el calor del cuerpo de un intruso.

"Infra" significa que la energía emitida está por debajo de la porción visible del espectro electromagnético. "Rojo" es el mas bajo nivel de la parte visible del espectro electromagnético que nuestros ojos pueden ver. Por lo tanto, "infrarrojo" significa: debajo del nivel de energía del color rojo, y aplica a muchas fuentes de energía invisible.

Un PIR está diseñado para activar una alarma cuando el detecta la imagen de un intruso, pero debe ser capaz de distinguir un intruso de otra fuente de energía infrarroja. La imagen detectada por un infrarrojo pasivo demuestra que la cabeza y el pecho son mas calientes que el resto del cuerpo. Esta distribución de la energía térmica en el cuerpo humano, como también el tamaño, ayuda a distinguir la "firma humana" de otras imágenes.

Si el intruso fuera la única imagen infrarroja que el PIR podría ver, la detección seria muy simple. Pero este no es el caso. El aire forzado procedente de un aparato, por ejemplo, crea imágenes sobre la pared similares a la imagen estacionaria del humano. El soplo de aire acondicionado sobre paredes a diferentes temperaturas causa un rápido cambio en temperatura y aparenta un movimiento en la superficie de la pared.

En la actualidad existen técnicas que emplean ópticas especiales para discriminar la imagen y detectar una figura humana sin posible error.

4.2.3.- Medios de seguridad en el control de acceso.

Además de los medios empleados en los controles de acceso de uso frecuente como arco detector, detectores manuales de metales, etc. Existen medios electrónicos de protección que autorizan o impiden el paso de forma automática a personas a las instalaciones.

Elementos como llave, aparatos emisores o tarjetas magnéticas identificativas que, combinadas con un elemento electrónico, autorizan o desautorizan el acceso a las instalaciones.

Entre estas ultimas tenemos las tarjetas perforadas Hollerith que son las mas antiguas y cuya lectura de su código se efectúa mediante perforaciones, pero presentaban el problema de su fácil falsificación y fueron excluidas.

Las tarjetas de banda magnética son más modernas e incorpora una banda magnética capaz de almacenar información en forma de código que insertada en un lector electrónico permite el acceso a las instalaciones.

4.2.4.- La seguridad biométrica.

El concepto biometría proviene de las palabras bio (vida) y metría (medida), por lo tanto con ello se infiere que todo equipo biométrica mide e identifica alguna característica propia de la persona.

La biometría es una tecnología de seguridad basada en el reconocimiento de una característica de seguridad y en el reconocimiento de una característica física e intransferible de las personas, como por ejemplo la huella digital.

Los sistemas biométricos incluyen un dispositivo de captación y un software biométrico que interpreta la muestra física y la transforma en una secuencia numérica. En el caso del reconocimiento de la huella digital, se ha de tener en cuenta que en ningún caso se extrae la imagen de la huella, sino una secuencia de números que las representan. sus aplicaciones abarca un gran número de sectores: desde el acceso seguro a computadoras, redes, protección de ficheros electrónicos, hasta el controlar y control de acceso físico a una sala de acceso restringido.

Por esta razón la definen como una rama de las matemáticas estadísticas que se ocupa del análisis de datos biológicos y que comprende temas como población, medidas físicas, tratamiento de enfermedades y otros por el estilo.

Todos los seres humanos tenemos características morfológicas únicas que nos diferencian. La forma de la cara, la geometría de partes de nuestro cuerpo como las manos, nuestros ojos y tal vez la más conocida, la huella digital, son algunos rasgos que nos diferencian del resto de seres humanos.

La medición biométrica se ha venido estudiando desde tiempo atrás y es considerada en la actualidad como el método ideal de identificación humana.

La identificación por medio de huellas digitales constituye una de las formas más representativas de la utilización de la biometría. una huella digital está formada por una serie de surcos. Las terminaciones sobre importaciones de los mismos son llamados "puntos de minucia". Cada uno de estos puntos tiene una característica y una posición única, que puede ser medida. Comparando esta distribución es posible obtener la identidad de una persona que intenta acceder a un sistema en general.

Con el atentado del 11-S contra las Torres Gemelas como 1 de los puntos de inflexión, al igual que posteriores atentados en Europa, el interés de la sociedad por utilizar patrones biométricos para identificar o verificar la autenticidad de las personas ha sufrido un aumento drástico en el sistema, que se refleja no solamente en novelas, películas y series de televisión, sino también en la aparición de diversas aplicaciones prácticas. Ya no nos es extraño oír hablar de pasaportes y carnés de identidad que incluyen características biométricas, si bien es cierto que siempre habían incluido dos de ellas: la foto del rostro y la huella dactilar. También comienza a ser frecuente la asistencia del sistema de acceso a instalaciones, ordenadores y teléfonos móviles mediante huella dactilar, para cajeros automáticos mediante iris, la utilización forense del reconocimiento de la escritura, voz y firma, estando presente en el campo de la medicina moderna…

La tarjeta de proximidad permite la lectura de su código consola aproximarla al equipo lector.

la tarjeta de infrarrojo nos permite la lectura de su código mediante sistemas ópticos o de lectura con luz infrarroja, activando el sistema en caso de ser reconocido su código como idóneo. Son de gran fiabilidad.

Las tarjetas de inducción son de las primeras que salieron al mercado y su funcionamiento se basa en la escritura de su código mediante pequeños elementos metálicos

embutidos en su interior, que produce la interrupción del campo magnético y como consecuencia de ello su interpretación binaria.

En la estructura de las actuales tarjetas figura un pequeño microchip que se utiliza como soporte de los datos el cual va a ser interpretado al ser pasados por el lector. Presenta la ventaja de una mayor cantidad de información que pueda ser almacenada.

4.2.5.- Fiabilidad de los sensores.

No todos los sensores tienen la capacidad de ser sensibles a todo tipo de actividad delictiva, puesto que la mayoría de los estudiados y los existentes en el mercado tienen fallos tales como: zonas sin cubrir como el subsuelo, falta de sensibilidad, envejecimiento del sensor, fácil sabotaje, etc.

Por otro lado todos ellos producen, con mayor o menor frecuencia, falsas alarmas: el paso de animales, inclemencia meteorológica, estamos bruscos de temperatura y humedad, acoplamiento otros aparatos instalados en el lugar… por lo que los policías locales frecuentemente nos vemos obligados a acudir a comprobarlas con la consiguiente pérdida de tiempo que ello supone, No obstante la experiencia y el conocimiento de cada 1 de los sensores que tenemos a nuestro cuidado nos hará conocer casi con toda certeza si se trata de una verdadera o falsa alarma.

4.2.6.- La centralita de alarma.

Cada sistema de seguridad (cada elemento instalado en la Jefatura) está conectado a una pequeña central remota que recibe identificados vial salto de la alarma a la central receptora.

La encargada de centralizar todos los elementos del sistema de seguridad instalado en un recinto cerrado y contiene el circuito correspondiente y la batería que mantendrá el sistema de funcionamiento en caso de fallo en el suministro eléctrico, puede ser con conexión por cableado o vía radio.

Como norma general y aunque la dependencia sea municipal y se trate de la Jefatura de la Policía Local, todo el sistema de centralización de alarma se estudia en el Reglamento de Seguridad Privada, quién establece que hay que tener en cuenta relacionado con los sistemas de seguridad los siguiente:

- El sistema debe contar con al menos 3 sensores, 1 primarios y 2 secundarios.
- La transmisión telefónica bidireccional será obligatoria en todos los sistemas.

- Todos los sistemas están sujetos a un chequeo anual. en caso de que el sistema no esté conectado a una central autorizada, los chequeos deberán hacerse trimestralmente por una empresa de seguridad.
- Las instalaciones conectadas a una central autorizada no llevan normalmente una sirena externa, ya que está no están autorizadas son armas de 30 segundos.
- Las empresas de seguridad están obligadas a instruir a los usuarios sobre su funcionamiento del servicio instalado.
- Los medios materiales y técnicos, aparatos para mí dispositivos de seguridad que instalen y utilicen estas empresas, habrán de encontrarse debidamente aprobados con arreglo a las normas que se establezcan, impidiendo que los sistemas de seguridad instalados causen daños o molestias a terceros.
- Los dispositivos Exteriores, tales como cajas de avisadores acústicos u ópticos, deberán incorporar el teléfono de contacto desde el que se pueda adaptar la decisión adecuada, y el nombre y teléfono de la empresa que realice su mantenimiento.
- Las empresas instaladoras de mantenimiento deberán disponer del servicio técnico adecuado que permita atender debidamente las averías de los sistemas de seguridad **de cuyo mantenimiento se hayan responsabilizado, incluso en días festivos, en el plazo de 24 horas siguientes al momento en el que hayan sido debidas al efecto.**

5.- EL CIRCUITO CERRADO DE TELEVISIÓN (CCTV).

5.1.- CCTV.

Actualmente se conoce como circuito cerrado de televisión al sistema de transmisión de imágenes compuesto básicamente por un número finito de cámaras y monitores en el cual se transmiten señales de las primeras dos segundos y que forman un conjunto cerrado y limitado, puesto que solo los componentes de dicho grupo pueden compartir tales imágenes, a diferencia de la televisión abierta pública, donde todo aquel que disponga de un receptor de video puede recibir la señal correspondiente.

El uso más común donde se aplica el circuito cerrado de televisión es el de la vigilancia y seguridad, pero existen otros campos donde también se utiliza como: control de tráfico, vigilancia del niño en guardería, control de líneas de producción…

Debido al gran crecimiento de los sistemas de CCTV, la industria desarrollado una gran variedad de equipamiento relacionado tales como grabadores digitales de vídeos, cámaras infrarrojas y servidores de cámara web que utilicen internet para vigilancia remota.

El diseño de un sistema de CCTV está regido por 5 cuestiones fundamentales:

- Determinación del propósito del sistema de CCTV.
- Definición del área que debe visualizar cada cámara.
- Determinación de la ubicación del o los monitores.
- Definición de la forma de transmisión de la señal de vídeos de las cámaras al monitor.

En base a los puntos anteriores, determinación del equipamiento necesario, escogiendo un sistema de observación o sistema profesional.

Asimismo, el CCTV permite ver y seguir la actividad del intruso o causa de la alarma y grabar las imágenes ante la posibilidad de poder ser empleada como prueba.

Durante la noche las zonas a cubrir por las cámaras están iluminadas por proyectores de luz blanca o infrarroja.

En la actualidad circuito cerrado de televisión utilizan el sistema denominado divisor de cuadrante mediante el cual no es necesario el empleo de un monitor por cámara, sino que una sola pantalla puede representar imágenes de distintas cámaras.

Dentro de un sistema de seguridad resulta muy importante el poder distinguir en el centro de control de las imágenes de las áreas más conflictivas; con ello se consiguen una serie de ventajas como son:

- Reducir el personal de seguridad.
- Aminora los riesgos físicos para dicho personal.
- Disuadir al posible agresor, al sentirse vigilado.
- Verificar al instante la causa de una alarma.
- Identificar al intruso.

5.2.- PARTES DE LAS CUALES SE COMPONE UN SISTEMA DE SEGURIDAD.

a) Elementos captadores de imágenes (camaras).
b) Elementos reproductores de imagen (monitores).
c) Elementos grabadores de imagen.

d) Elementos transmisores de la señal de video.
e) Elementos de control.
f) Vídeos sensores.

5.3.- EL CCTV Y SU UTILIZACIÓN EN LA VIDEOVIGILANCIA.

5.3.1.- Generalidades.

Para esta aplicación el circuito estará compuesto a parte de las cámaras y monitores, de un dispositivo almacenamiento de vídeos, dependiendo de la estructura del circuito ya sea analógico o basado en redes IP, aunque se pueden realizar combinaciones dependiendo de las necesidades del sitio.

Obviamente, además del concepto del servicio de videovigilancia y su finalidad, también se establecen los requisitos sobre su utilización, autorizaciones, monitorización…

"Los servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas".

"No tendrán la consideración de servicio de videovigilancia la utilización de cámaras o videocámaras cuyo objeto principal sea la comprobación del Estado de instalaciones o bienes, el control de accesos a aparcamientos y garajes, o las actividades que desarrollan desde los centros de control y otros puntos, zonas o áreas de las autopistas de peaje. Estas funciones podrán realizarse por personal distinto del de seguridad privada o Seguridad Pública".

Se limita el uso de cámaras o videocámaras con fines de seguridad privada en vías y espacios públicos o de acceso público, salvo autorización administrativa pero no competente en cada caso. caso de utilización en el interior de los domicilios se requerirá el consentimiento de su titular.

La autorización administrativa no será necesaria para el caso de las camas que formen parte de medidas de seguridad obligatorias.

Las grabaciones solo podrán destinarse a su uso en seguridad y con sometimiento a lo previsto en la normativa sobre materia de Protección de Datos de carácter personal.

5.3.2.- Cámaras I.P.

I.P. Internet Protocol (Protocolo de Internet). Protocolo de direccionamiento que se encarga de dirigir la información adecuadamente a través de la red. También: Protocolo para la comunicación en una red a través de paquetes conmutados, es principalmente usado en internet.

Las cámaras de I.P., de vigilancia que tienen la particularidad de enviar las señales de video y si necesita inclusive audio, pudiendo estar conectadas directamente a un router ADSL, o bien a un concentrador de una red local, para poder visualizar en directo las imágenes bien dentro de una red local (LAN), OA través de cualquier equipo conectado a internet (WAN) pudiendo estar situado en cualquier parte del mundo.

A la vez, las cámaras I.P. permiten el envío de alarmas y por medio de email, la grabación de secuencias de imágenes y de fotogramas, en formato digital en equipos informáticos situados tanto dentro de una LAN como de la WAN, permitiendo de esta forma verificar posteriormente lo que ha sucedido en el lugar o lugares vigilados por estos sistemas.

Las cámaras I.P. y los servidores de video disponen de software interno de apartados de seguridad que permiten generar establecer diferentes niveles de seguridad en el acceso a las mismas, siendo estos:

- *Administrador:* Acceso mediante Nombre de usuario y contraseña a la configuración total de las cámaras.
- *Usuario:* Acceso mediante Nombre de usuario y contraseña a la visualización de las imágenes y manejo del relé de salida.
- *Demo:* Acceso libre a la visualización sin necesidad de identificación, con accesos restringidos.

6.- FIABILIDAD Y VULNERABILIDAD AL SABOTAJE.

6.1.- CONCEPTO.

El verdadero fundamento de este tipo de protección, o mejor dicho elemento de la misma, es la detección y transmisión, ya que mediante sus alarmas y dispositivos de visión puede ser transmitido por procedimientos variados al elemento humano dentro de la protección.

Por ello dependiendo del equipo de trabajo que forman dichos elementos activo, junto a los elementos pasivos y humanos, para que la vulnerabilidad y eficacia del mismo se lleve a efecto o no en mayor o menor porcentaje.

La vulnerabilidad de este tipo de medios están en mayor o menor peligro de ataque que pueda sufrir alguno de sus componentes o mecanismos externos por medio de cualquier agente agresor.

6.2.- PROTECCIÓN DE LA CÁMARA IP.

Una cámara I.P., al igual que los servidores de video, dispone de un software interno sobre el tema de seguridad, que nos permiten establecer el nivel de seguridad sobre el acceso:

- *Administrador:* Acceso mediante Nombre de usuario y contraseña a la configuración total de las cámaras.
- *Usuario:* Acceso mediante Nombre de usuario y contraseña a la visualización de las imágenes y manejo del relé de salida.
- *Demo:* Acceso libre a la visualización sin necesidad de identificación, con accesos restringidos.

7.- CONCLUSIÓN.

Vivimos en una continua amenaza terrorista, nos encontramos en un nivel 4 antiterrorista, mas todos los ataques que podamos recibir de personas normales, todos aquellos elementos de seguridad que podamos exigir a la administración en nuestras despendencias, y que nos sirvan para proteger tanto éstas, como para nuestra propia integridad física, es poco, puesto que si se pierde el trabajo se sigue vivo, pero si perdemos la vida, o nuestro psique por una mala intervención y proteccion, perdemos nuestra identidad.

8.- BIBLIOGRAFÍA:

GONZALEZ LEZCANO , R.A; ECHEVERRIA TRUEBA, J.B << Seguridad en caso de incendio

Para diseñadores de edificios.

CEP << Manual Seguridad en edificios públicos. Formación para el empleo.

OLLEROS A. << Libro Arquitectura y Seguridad en Proyectos Edificación.

https://publicaciones.defensa.gob.es/libros/colecciones/documentos-de-seguridad-y-defensa-edificios-militares-singulares/sort-by/name/sort-direction/asc.html