



**MANUAL
DE RECOMENDACIONES
EN MATERIA DE SEGURIDAD
EN LOS COMERCIOS
ANDALUCES**



CEA Confederación de
Empresarios de Andalucía



JUNTA DE ANDALUCÍA
CONSEJERÍA DE TURISMO, COMERCIO Y DEPORTE

ÍNDICE.

1. INTRODUCCIÓN.

2. POSIBLES DAÑOS Y PÉRDIDAS.

2.1. DAÑOS Y PÉRDIDAS DE CARÁCTER ANTISOCIAL.

- 2.1.1. PÉRDIDA DESCONOCIDA.
- 2.1.2. ROBO.
- 2.1.3. FRAUDE Y ESTAFA.
- 2.1.4. FALSIFICACIÓN DE MONEDA.
- 2.1.5. AGRESIÓN PERSONAL.
- 2.1.6. ACCIÓN VANDÁLICA.
- 2.1.7. RIESGOS DE INTERNET.

2.2. DAÑOS Y PÉRDIDAS DE CARÁCTER TÉCNICO Y LABORAL.

- 2.2.1. INCENDIO O COMBUSTIÓN.
- 2.2.2. AVERÍAS.
- 2.2.3. ACCIDENTES.
- 2.2.4. MANIPULACIÓN DE PRODUCTOS.
- 2.2.5. INADECUADA PROTECCIÓN DE DATOS.

3. SISTEMAS DE SEGURIDAD DISPONIBLES.

3.1. SISTEMAS DE SEGURIDAD PASIVA.

- 3.1.1. CONTROL DE ACCESOS.
- 3.1.2. PROTECCIÓN CONTRA HURTO, ROBO Y ATRACO.
- 3.1.3. PROTECCIÓN ANTE LA AGRESIÓN.
- 3.1.4. PROTECCIÓN DE INFORMACIÓN Y VALORES.
- 3.1.5. PROTECCIÓN CONTRA INCENDIOS.

- 3.1.6. EXTINCIÓN DE INCENDIOS.
- 3.1.7. EMERGENCIA Y EVACUACIÓN.
- 3.2. SISTEMAS DE SEGURIDAD ACTIVA.
 - 3.2.1. CONTROL DE ACCESOS E IDENTIFICACIÓN.
 - 3.2.2. PROTECCIÓN CONTRA HURTO, ROBO Y ATRACO.
 - 3.2.3. PROTECCIÓN ANTE LA AGRESIÓN.
 - 3.2.4. PROTECCIÓN DE INFORMACIÓN Y VALORES.
 - 3.2.5. PROTECCIÓN CONTRA INCENDIOS.
 - 3.2.6. EXTINCIÓN AUTOMÁTICA.
 - 3.2.7. CONTROL Y EMERGENCIA.

4. RECOMENDACIONES SOBRE SEGURIDAD.

- 4.1. RECOMENDACIONES GENERALES.
- 4.2. SEGURIDAD EN EL EXTERIOR DEL LOCAL.
 - 4.2.1. PUNTOS DE ACCESO AL LOCAL.
 - 4.2.2. APERTURA Y CIERRE.
 - 4.2.3. ALARMAS EXTERIORES.
 - 4.2.4. VIDEOVIGILANCIA EXTERIOR.
 - 4.2.5. INGRESOS DE EFECTIVO EN ENTIDADES FINANCIERAS.
 - 4.2.6. RELACIONES CON OTROS AGENTES.
- 4.3. SEGURIDAD EN EL INTERIOR DEL LOCAL.
 - 4.3.1. CAJAS REGISTRADORAS.
 - 4.3.2. BILLETES DE EURO.
 - 4.3.3. CAJAS FUERTES.
 - 4.3.4. VIDEOVIGILANCIA INTERIOR.
 - 4.3.5. ILUMINACIÓN INTERIOR.
 - 4.3.6. PRODUCTOS COMERCIALIZADOS.
 - 4.3.7. CLIENTES Y EMPLEADOS.

4.4. SEGURIDAD Y NUEVAS TECNOLOGÍAS.

4.4.1. TARJETAS DE CRÉDITO Y DÉBITO.

4.4.2. INTERNET.

4.4.3. PROTECCIÓN DE DATOS.

4.5. DURANTE Y DESPUÉS DEL HECHO DELICTIVO.

4.5.1. DURANTE EL HECHO DELICTIVO.

4.5.2. DESPUÉS DEL HECHO DELICTIVO.

ANEXO. NORMATIVA SOBRE SEGURIDAD PRIVADA.



1. INTRODUCCIÓN.

La Confederación de Empresarios de Andalucía viene manteniendo una estrecha interlocución con la Consejería de Turismo, Comercio y Deporte de la Junta de Andalucía y, en concreto, con la Dirección General de Comercio. Dicha interlocución está sustentada en los sucesivos acuerdos de concertación social, el último del los cuales, VII Acuerdo de Concertación Social de Andalucía, fue firmado el 24 de noviembre de 2009 por el Presidente de la Junta de Andalucía, el Presidente de CEA y los secretarios generales de las centrales sindicales mayoritarias.

Constituye un hecho constatable que la negativa coyuntura económica actual ha provocado un considerable incremento de los robos, hurtos y hechos delictivos durante el pasado año 2009, con especial repercusión en los establecimientos comerciales andaluces.

Tal es así, que la Confederación de Empresarios de Andalucía ha incluido en el VII Acuerdo de Concertación Social de Andalucía, actuaciones orientadas a incrementar la calidad y seguridad en los establecimientos comerciales, lo que se va a traducir en el nuevo Plan Integral de Fomento del Comercio Interior de Andalucía, como una de las líneas fundamentales de actuación.

Asimismo, de forma bipartita la CEA también mantiene una estrecha relación de cooperación con la Dirección General de Comercio, que se materializa a través de sucesivos convenios de colaboración que incluyen programas concretos de actuaciones de fomento e impulso del sector comercial andaluz. En este sentido, en el programa de actividades del convenio de colaboración firmado con fecha 8 de junio de 2009 se ha incluido una actividad consistente en la elaboración de un **"Manual de Recomendaciones en Materia de Seguridad en los Comercios Andaluces"**, a fin de minimizar los perjudiciales efectos que sobre el comercio está teniendo el aumento de la actividad delictiva como consecuencia de la crisis económica en la que estamos inmersos, entre otras causas destacables.

Para la elaboración técnica del manual la Confederación de Empresarios de Andalucía ha contado con la colaboración directa de la Confederación Empresarial de Comercio de Andalucía, CECA, organización sectorial representativa del comercio

tradicional en Andalucía. Con carácter previo a la elaboración del manual, se han desarrollado unas sesiones técnicas de trabajo en cada provincia, a fin de tomar un contacto real con la actividad comercial a modo de "Brainstormings" o tormenta de ideas.

En conclusión, el manual recoge una serie de medidas y recomendaciones en materia de seguridad en los comercios andaluces, elaborado en base a las necesidades e inquietudes reales que en esta materia tienen los comerciantes andaluces. De igual modo, para un mejor y más práctico uso del contenido del citado manual se ha elaborado un **tríptico informativo** en el que se explica, de forma resumida, las principales recomendaciones contenidas en el manual.



2. POSIBLES DAÑOS Y PÉRDIDAS

2.1 DAÑOS Y PÉRDIDAS DE CARÁCTER ANTISOCIAL

2.1.1 PÉRDIDA DESCONOCIDA

Entre los muchos elementos que determinan el precio de venta de los artículos expuestos en los establecimientos comerciales, la pérdida desconocida es uno de los componentes intrínsecos menos analizado pese a los altos costes que ello representa.

La pérdida desconocida es un concepto que integra el hurto interno, el hurto externo y los errores en la administración del establecimiento comercial. Se identifica como consecuencia de mecanismos de gestión por comparación, como son los inventarios de almacén o la acción diaria de cuadre de las cajas de los puntos de venta y la comprobación de los históricos. Esta pérdida incide directamente en los beneficios empresariales.

Pero definamos primero lo que se considera **hurto**. Este acto consiste en apropiarse, tomando una cosa mueble ajena, sin la voluntad de su dueño. Está caracterizado por el ánimo de lucro.

• Hurto interno

Analizando las estadísticas españolas sobre este tema, se distinguen varios supuestos: empleados que roban habitualmente, empleados que robarían si tuviesen oportunidad y empleados que no robarían en absoluto. Es entendible el grave problema con el que se encuentran los responsables de los establecimientos. Algunos de los hurtos más frecuentes se producen en la línea de cajas por: escaneo falso de productos o falta de registro de precios; anulaciones fraudulentas, falsas devoluciones a los clientes; registros de precios inferiores o de otros departamentos al de los artículos, entrega de cambio de menos a los clientes, etc.

• Hurto externo

Los focos de este tipo de delito se localizan en el área comercial y en los almacenes y son producidos, normalmente, por clientes y proveedores. Ejemplos de productos que más se “descuidan” son bebidas (normalmente alcohólicas) y tabacos.

En algunas de las secciones de los establecimientos comerciales se ha reducido este problema mediante la utilización de dispositivos antihurto y de antenas detectoras.

- **Errores administrativos**

Igualmente, al final del día se producen diferencias en el arqueo de las cajas y en los históricos de venta diaria, producidos normalmente por errores humanos –no intencionados– en la introducción de unidades de producto y cantidades.

Este riesgo, aunque no está directamente relacionado con la seguridad, es un riesgo propio de la actividad comercial a tener en cuenta y su reducción debe ser uno de los objetivos a conseguir cuando se intente adoptar una verdadera política integral de prevención de pérdidas en los establecimientos comerciales.

TIPO DE HURTOS MÁS USUALES

- **Chicle:** este tipo de hurto se da sobre todo en joyerías. El delincuente pega un chicle bajo el mostrador y cuando le muestran las piezas, hurta una y la pega en el chicle. Si el trabajador se percata, el delincuente niega haberlo hecho y no se puede proceder en su contra. Si el trabajador no se percata, posteriormente un cómplice recoge la pieza pegada al chicle.
- **Capote:** uno de los delincuentes hace salir de detrás del mostrador al trabajador y con una bolsa de grandes dimensiones o similar obstruye la visión del mostrador al trabajador, momento que el otro delincuente aprovecha para acceder a la parte posterior del mostrador y sustraer dinero u objetos.



- **Pañuelo:** el delincuente simula estar resfriado y con una tos muy fuerte. Con la ayuda de un pañuelo hurta los objetos.
- **Bolsa con el interior recubierto de papel de aluminio:** estas bolsas de fabricación casera evitan el funcionamiento de los chips de seguridad instalados en los artículos, al pasar por el arco detector de la puerta del establecimiento.
- **Distracción del trabajador:** los delincuentes actúan en grupo y, mientras unos distraen y engañan al vendedor, otros consuman el hurto.
- **Mancha:** este tipo de hurto no afecta directamente al establecimiento pero sí a los clientes y, en muchas ocasiones, el hecho ilícito se inicia en el establecimiento comercial. En este caso los delincuentes también actúan en grupo, y consiste en que uno de ellos tira un líquido (café, chocolate, etc.) sobre la ropa de la víctima y enseguida le ofrece ayuda para limpiarle, mostrándose muy preocupado y dando excusas de forma reiterada. Este descuido es aprovechado por un segundo delincuente para consumir el hurto.

2.1.2 ROBO

El robo consiste en apoderarse, con ánimo de lucro, de una cosa mueble ajena empleando fuerza en las cosas para acceder al lugar donde ésta se encuentra o con violencia o intimidación en las personas.

El comúnmente conocido atraco consiste en apoderarse de la cosa mediante violencia física o psicológica. Es una variedad de robo **con violencia e intimidación a las personas**. Se comete, en mayor medida, en establecimientos y/o recintos donde se maneja dinero o en los trayectos hacia éstos.

En los establecimientos comerciales el atraco, se comete en las pequeñas tiendas sin vigilancia en las que el atracador ocasional encuentra un fácil botín y una huida rápida, en recintos protegidos de conteo de efectivo, o durante el traslado de fondos en donde una banda organizada acecha para llevarse un gran botín.

TIPO DE ROBOS MÁS USUALES

En caso de fuerza sobre las cosas:

- Escalamiento.
- Rompimiento de paredes, techo o suelo, o fractura de puerta o ventana.
- Fractura de armarios, muebles u objetos cerrados, forzamiento de sus cerraduras.
- Empleo de llaves falsas.
- Inutilización de sistemas específicos de alarma o guarda para acceder al lugar donde se encuentre el objeto.

En caso de violencia o intimidación sobre las personas:

- El robo con violencia se da cuando se ejerce fuerza física sobre las personas con el fin de conseguir apoderarse de una cosa que ellas poseen.
- En el robo con intimidación, el apoderamiento de una cosa se da cuando se produce el hecho con amenaza de causar dolor a la persona que posee la cosa. Esta amenaza se puede realizar de manera verbal o mediante armas u objetos peligrosos.

2.1.3 FRAUDE Y ESTAFA

Fraude es todo engaño o acción de mala fe ejecutados con el fin de procurarse un beneficio ilícito en perjuicio y a expensas de otro. También el acto o efecto de lesión que se causa en el patrimonio ajeno de forma no violenta, por medio de engaño y con intención de lucro.



El fraude que se puede detectar en estos establecimientos comerciales se da principalmente en los medios de pago, habitualmente cuando se realiza el abono de la cuenta con tarjeta de crédito sustraída o encontrada. En estos casos, el presunto estafador intentará imitar la firma del propietario y aportará un carné falsificado con esta misma firma. Posteriormente, el verdadero propietario negará haber realizado la compra y, por tanto, se negará a abonarla, con la consiguiente pérdida para el establecimiento comercial.

Estafa, por el contrario, consiste en pedir o sacar dinero o cosas de valor con artificios o engaños. Podemos destacar los cheques al portador en efectivo, cheques manipulados y falsificación de documentos mercantiles. También se entraría dentro de la estafa el valerse de alguna manipulación informática y conseguir la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero, entre otros.

Este riesgo es de especial consideración para los gerentes de los pequeños comercios.

TIPO DE ESTAFAS MÁS USUALES

- En el **pago**: el estafador compra un objeto pagando con un billete de gran valor y engaña al comerciante para quedarse con el billete y el cambio. Si la persona únicamente distrae de alguna forma al comerciante y coge el billete con el que había pagado no se tratará de estafa sino de hurto.
- Hay que vigilar las **monedas**, las hay de países asiáticos que se parecen a los euros pero que no son de curso legal ni tienen el mismo valor.
- **Cambio de códigos de barras**: consiste en cambiar el código de barras de artículos de precio elevado por el código de barras de artículos más baratos.
- **Billete cliché**: el estafador presenta unos papeles negros (negativos) que cuando les aplica un líquido revelador se transforman en billetes.
- **Estafa telefónica**: el estafador llama al comerciante y le engaña haciéndole creer que ha ganado algún premio o similar, y que para obtenerlo debe llamar a un número de teléfono de tarifa elevada (803, 806, 807).

- **Cajero bloqueado o manipulado:** el estafador manipula o instala una boca de cajero falsa encima de la boca original del cajero.
- Timo conocido vulgarmente como “**carta nigeriana**”: carta que normalmente se recibe por correo electrónico y propone a quien la recibe participar en un lucrativo negocio, ordenando transferencias a una cuenta extranjera, y ofreciendo un porcentaje de cada una de ellas en concepto de beneficios. Quien las envía normalmente dice ser heredero de algún rico empresario, agraciado por algún premio de lotería, etc. y pide ayuda para sacar dinero del país.
- **Phishing:** estafa a través de Internet con simulación de páginas de bancos, cajas y otras entidades financieras. Se explicará más detenidamente en la sección sobre riesgos de Internet.

2.1.4 FALSIFICACIÓN DE MONEDA

La falsificación de moneda es uno de los riesgos a tener muy en cuenta ya que su materialización incide directamente en la cuenta de resultados. Este tipo de acciones delictivas tiene su escenario precisamente en establecimientos donde exista un gran movimiento de efectivo y de personas que hagan muy difícil su detección y localización.

En los billetes de euro existen diferentes medidas de seguridad que previenen la falsificación y que son fácilmente identificables a simple vista o mediante la aplicación de luz ultravioleta.

2.1.5 AGRESIÓN PERSONAL

Consiste principalmente, a un nivel inferior, en la realización de intimidaciones, altercados y amenazas entre el personal del establecimiento comercial y clientes o entre compañeros por motivos laborales, y



a un nivel de dueños de establecimientos y altos directivos de grandes formatos comerciales, en extorsiones y secuestros con la intención de causarles daño a ellos o a su familia en su persona, imagen o propiedad.

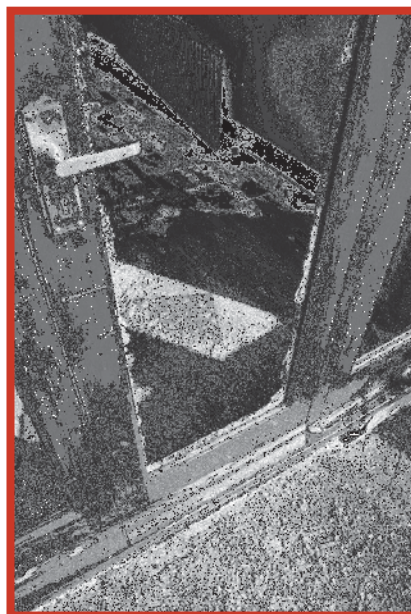
En los formatos comerciales de cierto tamaño el riesgo de agresión personal conviene señalarlo como fuente de malestar dentro de la plantilla.

2.1.6 ACCIÓN VANDÁLICA

Las acciones vandálicas son destrucciones o deterioros intencionados de los bienes, normalmente producidos en el exterior de las instalaciones de los establecimientos comerciales, los más frecuentes son: rotura de cristales, destrucción y apertura de embalajes, desperfectos en fachada, pintadas, *graffitis*, encartelamientos, destrucción de rótulos y atrancamiento de puertas y cerraduras.

Las personas, empleados y clientes, no suelen verse afectados por estos daños que, normalmente, son producidos fuera del horario laboral, la mayoría de las veces se producen como consecuencia de manifestaciones, tumultos y reivindicaciones sociales y laborales no satisfechas.

La acción vandálica tiene especial incidencia en las zonas comunes: aseos, zonas de tránsito, calles comerciales por lo que deberá ser analizado por el Director de Seguridad.



2.1.7 RIESGOS DE INTERNET

VIRUS, GUSANOS Y ATAQUES DE INGENIERÍA SOCIAL

Podemos encontrar en Internet un conjunto de programas, denominados en su conjunto "**malware**" o software malicioso, que son creados con la intención principal

de provocar daños, utilizar los recursos de los usuarios o recabar información de utilidad para los creadores o usuarios de los mismos.

Por otro lado, Internet es también zona de práctica para aquellos que aplican técnicas de **ingeniería social** con el objetivo de recabar información relevante de los usuarios que pueda ser utilizada para obtener algún tipo de beneficio, generalmente económico. Entre estas prácticas están de plena actualidad las conocidas como "*phishing*" y "*pharming*", cuyos ataques están alcanzando gran nivel de virulencia provocando importantes daños en sectores como la banca en línea en Internet.

Los "**virus**" son programas que, incorporados en ficheros ejecutables o con formatos de uso común por los sistemas operativos habituales, logran acceso al sistema con la finalidad de ejecutarse y, en la mayoría de los casos, reproducirse mediante copia que se aloje en otros ficheros o en otros sistemas. El nivel de peligrosidad de los virus se establece en función de los daños que es capaz de producir en el sistema - desde la aparición de mensajes hasta la total destrucción de la información de los equipos infectados - y de su velocidad y facilidad de propagación. Su desarrollo y creación tienen mucho que ver con las vulnerabilidades existentes en el software de uso común, por lo que una primera barrera de prevención la encontraremos en mantener actualizado y al día nuestro sistema, además de utilizar herramientas de detección y desinfección. Además, hoy en día existen numerosos servicios públicos donde podremos encontrar cumplida información sobre cualquier virus, además de información sobre cómo prevenir sus ataques.

El término "**gusano**", o "gusano de Internet", denomina a aquellos programas diseñados para ser capaces de trasladarse a través de redes de ordenadores con el fin de realizar una actividad concreta incorporada en su código. Aunque su finalidad no tiene en principio que entrañar peligro, estos programas pueden instalar un virus, instalar un programa que actúe en segundo plano sin conocimiento del usuario, o dedicarse a consumir ancho de banda del sistema utilizándolo para realizar acciones como el envío masivo de correo electrónico.

En cuanto a los "**troyanos**" o "caballos de Troya" son, como su propio nombre indica, programas que simulan realizar una función distinta a aquella para la que han sido diseñados, y que entran en el sistema bajo el disfraz de software útil para el

usuario. Una variante de éste tipo de software malicioso son las "bombas lógicas", programas que permanecen inactivos en el sistema hasta que son activados por la ocurrencia de un evento o por el mero paso del tiempo, y que permanecen ocultos en el código del programa.

Podemos definir al "**phishing**" como una forma de ingeniería social en la que se intenta obtener de forma fraudulenta información sensible de una víctima suplantando la identidad de un tercero de confianza. El principal objetivo ha sido hasta el momento la información de acceso de usuarios de banca en Internet o sitios web dedicados a las subastas, en los que es factible tener acceso a cuentas bancarias y tarjetas de crédito. El cauce más habitual de difusión de estos ataques es el correo electrónico. Es habitual recibir mensajes remitidos supuestamente desde los servicios de atención al cliente de un banco que nos requieren, por ejemplo, la introducción de un código de usuario y su clave de acceso para "validarlos" en un formulario que simula ser parte del sitio web de una entidad financiera. Otra modalidad, de reciente aparición, es la que utiliza el canal telefónico, realizando una llamada al domicilio del usuario simulando hacerlo desde el Centro de Atención al Cliente de un Proveedor de Servicios de Internet y solicitando al usuario que introduzca datos de carácter personal en un formulario colocado en un sitio Web controlado por los atacantes.

En cuanto al "**pharming**", de mayor complejidad técnica en su desarrollo, podemos decir que trata de conducir al usuario a un sitio web simulado, alterando bien los servidores del sistema de nombres de dominio de Internet (DNS) o bien manipulando ficheros en los equipos de los usuarios con la finalidad de que redirijan las peticiones de acceso a determinados sitios web a otros sistemas controlados por el atacante.

BANCA Y COMERCIO ELECTRÓNICO

Los portales de comercio electrónico permiten la adquisición y venta de productos y servicios utilizando Internet como canal de comunicación. El usuario debe dedicar un pequeño esfuerzo en conocer los servicios y el tipo de información a que puede tener acceso. La existencia de políticas de privacidad comprensibles, la

identificación del responsable del servicio con todos los datos necesarios para localizarle y el uso de certificados electrónicos de identificación proporcionados por un tercero de confianza, la presencia de información sobre el modo de contratar o la utilización de conexiones seguras para facilitar los datos o gestionar los pagos, son datos que deben ser tenidos en cuenta antes de utilizar este tipo de servicios.

Para acceder a los servicios deberá **acreditar su identidad**. En la actualidad, el medio más extendido es la utilización de códigos de usuario y palabras de paso, aunque desde hace tiempo es posible utilizar certificados digitales expedidos por la Fábrica Nacional de Moneda y Timbre u otros proveedores de servicios de certificación. El DNI electrónico, que ya ha empezado a distribuirse, y que en breve estará disponible para todos los ciudadanos españoles, podrá ser utilizado para acreditar de forma fehaciente la identidad de un ciudadano en Internet.

2.2 DAÑOS Y PÉRDIDAS DE CARÁCTER TÉCNICO Y LABORAL

2.2.1 INCENDIO O COMBUSTIÓN

Un incendio es casi siempre inesperado y, normalmente, conlleva peligro para la integridad física de las personas y suele representar grandes pérdidas económicas por sus consecuencias devastadoras.

Los incendios fortuitos se producen en los establecimientos comerciales por diferentes causas: cortocircuitos eléctricos, descuidos, cigarrillos y cerillas mal apagadas, superficies calientes, sistemas de ventilación, calefacción y motores, etc.

Igualmente, los productos en mal estado, fermentados o un almacenaje inadecuado de productos inflamables pueden producir combustiones espontáneas.

2.2.2 AVERÍAS

Siguiendo con nuestra catalogación de los riesgos que pueden afectar a un centro comercial, deberemos detenernos en las averías de cualquier tipo que suponen un trastorno en la actividad diaria del complejo comercial. Un incompleto programa de conservación y mantenimiento, sin asignación de recursos técnicos y económicos,

disminuye la vida útil prevista para materiales, equipos y sistemas, provocando averías en las instalaciones primarias y secundarias.

La materialización del riesgo de avería suele causar un perjuicio económico elevado para cualquier actividad, tanto a nivel de imagen/marca, como en los beneficios. Las averías reiteradas provocan desidia en los empleados y pérdida de confianza en los clientes. Así, por ejemplo, un mal funcionamiento prolongado de la cámara frigorífica, echará a perder los alimentos perecederos provocando su falta de disponibilidad para los clientes; un escape de gas de los congeladores, puede causar intoxicaciones a empleados o clientes; la corrosión de los materiales puede causar envenenamiento de los alimentos; unos cables eléctricos pelados pueden causar cortocircuitos y electrocuciones y provocar incendios, etc. Todo ello se traduce en pérdidas para la empresa.

2.2.3 ACCIDENTES

Otro de los riesgos a considerar en este apartado de riesgos técnicos es el riesgo de accidente. El funcionamiento mecánico, hidráulico, eléctrico, termodinámico o electromagnético de la mayoría de las instalaciones que componen un centro comercial produce, con bastante frecuencia, electrocuciones, aplastamientos por puertas hidráulicas, atropellos con toros mecánicos, etc. Igualmente, las caídas fortuitas por resbalamiento en suelos deslizantes, derrames de productos o las intoxicaciones por la utilización de productos tóxicos de limpieza son algunos de los ejemplos de accidentes diarios que se pueden producir en la actividad comercial.

2.2.4 MANIPULACIÓN DE PRODUCTOS

Cada actividad industrial lleva asociada, por definición, su propio catálogo de riesgos laborales más o menos reducido. En algunos establecimientos comerciales, el tratamiento de



alimentos frescos y perecederos y la manipulación de productos tóxicos de venta o de mantenimiento hacen que este tipo de riesgo se convierta en especialmente relevante.

Así, por ejemplo en el área de almacenes y tienda, los riesgos sobre manipulación de productos a los que se encuentran expuestos los trabajadores pueden ser intoxicaciones por manipulación indebida de productos, lesiones en la espalda, levantamiento y transporte de cargas, inhalación de gases y polvos, hipotermias en las cámaras frigoríficas, golpes de calor en las panificadoras, virus, bacterias y hongos de fermentaciones, etc.

2.2.5 INADECUADA PROTECCIÓN DE DATOS

La Ley Orgánica de Protección de Datos (LOPD) obliga a toda persona física o jurídica que posea bases de datos o ficheros a implantar una serie de medidas técnicas y organizativas que garanticen la confidencialidad de estas informaciones. Esto supone que toda empresa que tenga datos de sus empleados, clientes, proveedores, etc., en función del contenido de los ficheros de datos, deben aplicar diferentes normas de seguridad.

Entre las medidas técnicas y organizativas a adoptar, es necesaria la creación de un documento de seguridad que describa los procedimientos del tratamiento informático de los ficheros, y garantizar los derechos de información y acceso a los datos por parte de los interesados. Es importante la inscripción de la existencia de los ficheros en el *Registro General de la Agencia de Protección de Datos (APD)*, un requisito formal que en absoluto presupone la adopción efectiva de las medidas de seguridad detalladas en la legislación.

La no adopción de ciertas medidas de seguridad puede suponer graves sanciones a la empresa, hasta llegar a los 601.000 euros.

La LOPD obliga a respetar el derecho a la intimidad de las personas que tiene su base en la Constitución Española y respetar la privacidad de los datos almacenados en los ficheros.

La ley establece tres niveles de medidas de seguridad (básico, medio, alto) las cuales deberán ser implantadas dependiendo de los distintos datos personales incluidos en el fichero (salud, ideología, religión, creencias, etc.).

- El **nivel básico** es cualquier conjunto de datos que se refieren a una persona identificada o identificable: nombre, apellidos, teléfono, etc.
- El **nivel medio** incluye datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y los servicios de solvencia y crédito.
- El **nivel alto** incluye datos de ideología, religión, creencias, origen racial, salud o vida sexual, así como los recabados para fines policiales sin consentimiento de las personas afectadas.

Lo habitual en el caso de pymes es tener una administración de empleados, cuya nómina puede incluir datos de carácter personal de nivel alto: el tipo de contrato utilizado, en términos de la Seguridad Social, desvela posibles discapacidades del propio empleado; además se recaba información para Hacienda de la discapacidad de personas que están a cargo de los empleados. También las posibles afiliaciones sindicales son datos personales de nivel alto.

Si dicho fichero está en manos de una gestoría o no, no cambia la obligación de notificarlo a la AEPD. Si la gestión del fichero es realizada por terceros (típicamente gestorías), se debe hacer constar qué gestoría se hace cargo del tratamiento de los datos. En la mayoría de pymes, los otros ficheros de datos personales sólo tienen datos de nivel básico. Aunque también deben ser declarados ante la agencia española de protección de datos, su nivel de protección es más fácil de cumplir.

Los usuarios que tengan permiso de acceso a datos de carácter personal, sólo deben poder acceder a los datos que sean relevantes y necesarios para ellos, para el desempeño de sus funciones. Para poder imponer esta exigencia, la empresa debe implantar un sistema de permisos de acceso; habitualmente se utilizan las funciones del sistema operativo.

Para ficheros de nivel medio y alto, también debe existir un control de acceso físico a los locales donde se encuentran los sistemas de información.

El responsable del fichero es el encargado de que exista en la empresa u organización una relación actualizada de usuarios y perfiles de usuarios y los accesos autorizados para cada uno de ellos.

Los soportes (cartuchos, cintas, disquetes, discos, CDS, DVD's, etc.) deben identificar el tipo de información que contienen. Los soportes tienen que ser inventariados, y almacenados con el acceso restringido. Cualquier salida de la empresa de datos de carácter personal debe ser autorizada por el responsable del fichero.



3. SISTEMAS DE SEGURIDAD DISPONIBLES

3.1 SISTEMAS DE SEGURIDAD PASIVA

Definimos genéricamente como **sistemas de seguridad pasiva** a aquellos materiales, equipos y sistemas de seguridad de carácter físico o mecánico, que se pueden emplear o se emplean específicamente para la prevención y la protección ante los riesgos y amenazas de los establecimientos comerciales. Entre los principales sistemas de seguridad pasiva, de aplicación a este tipo de actividad, se encuentran:

- **Control de accesos**
- **Protección contra hurto, robo y atraco**
- **Protección ante la agresión**
- **Protección de información y valores**
- **Protección contra incendios**
- **Extinción de incendios**
- **Emergencia y evacuación**

3.1.1 CONTROL DE ACCESOS

El control de accesos, en cuanto a medios técnicos pasivos se refiere, es el conjunto de dispositivos físicos y mecanismos que han de servir para identificar, inspeccionar y autorizar el paso o circulación de personas, vehículos y objetos hacia un área, para la prevención y protección ante riesgos que puedan afectar a las personas, los bienes y/o las instalaciones.

En función de su aplicación, el control de accesos puede ser: de personas, de vehículos y de objetos.

Entre los principales equipos y sistemas de seguridad pasiva para el control de accesos, de aplicación en establecimientos comerciales, se encuentran:

- **Las puertas blindadas**, de acceso a recintos protegidos.
- **Las puertas acorazadas**, de acceso a recintos protegidos.
- **Las cerraduras de seguridad**, para proteger el acceso a áreas restringidas.
- **Los sistemas de amaestramiento y jerarquización de llaves**, para la optimización y control de las cerraduras.
- **Los torniquetes**, para áreas de acceso a salida de público y personal.
- **Las barreras de control** de vehículos.

✓ **Puertas blindadas**

Las puertas blindadas se definen como elementos practicables para el cierre de huecos de paso, con especial función de control del acceso y protección ante la intrusión, sin función estructural, construidas mediante chapa de acero o maderas tratadas u otros materiales.

Aplicación. Las puertas blindadas están especialmente diseñadas para el cierre de huecos de paso en cerramientos interiores o exteriores con requerimientos de seguridad de grado medio.

La **tipología** de las puertas blindadas permite su clasificación general en:

- *Según el material:* maderas duras, maderas estratificadas, acero normal o especial, materiales sintéticos y materiales combinados.
- *Según su composición:* marco de puerta, hoja de puerta, sistema de anclaje, pestillería, apertura eléctrica/motor, cerraduras, sistema de bloqueo y sistema de alarma.
- *Según el grado de seguridad:* grado A –ataque con elementos manuales–, grado B –ataque con equipos mecánicos– y grado C –ataque con equipos térmicos–.

Para garantizar sus **condiciones de seguridad**, las puertas blindadas presentan una serie de características particulares para su montaje y recibido en muros y paredes:

- *Tipo de soporte:* la puerta presentará el mismo grado de seguridad que el muro o pared en el que vaya recibida.
- *Sistema de anclaje:* el sistema de anclaje o sujeción del marco o cerco es un elemento definitorio para la correcta o incorrecta forma de recibido de puertas al soporte o muro de cerramiento donde han de quedar solidariamente integradas. Cabe destacar los sistemas de recibido, así como la utilización de tornillos de expansión o procedimiento similar indismontable.
- *Material de recibido:* se utilizan generalmente morteros de cemento, con independencia de la soldadura previa a los anclajes o armaduras o sujeción o unión similar al anclaje marco-estructura soporte. Aglomerados o conglomerados sintéticos o hidráulicos especiales de alta resistencia y fraguado rápido, también son utilizados para el recibido de anclajes y marcos.

La **colocación y montaje** de las puertas blindadas requiere un planteamiento y ejecución ordenada y controlada con rigor como garantía de seguridad de la instalación. En el esquema general del proceso hay que prestar especial atención a:

- *Situación y disposición de las puertas:* sentido de apertura, mano de apertura y barrido del radio de giro.
- *Precauciones previas:* colocación del conjunto hoja-cerco o solamente cerco, posterior a la terminación de la obra de fábrica o de hormigón. Comprobar medidas de marcos y cercos, holguras, anclajes y apertura de la hoja en todo su radio de giro.

✓ **Puertas acorazadas**

Las puertas acorazadas se definen como elementos practicables para el acceso al recinto delimitado por los muros y forjados acorazados. Su grado de seguridad debe ser, como mínimo, el mismo que el del muro.

Aplicación. Las puertas acorazadas son de aplicación para su instalación en el acceso a la cámara acorazada y recintos protegidos.

La **tipología** de las puertas acorazadas permite su clasificación general en:

- *Según su maniobra:* abatible, giratoria con eje lateral y giratoria con eje central.
- *Según el material de defensa:* acero tradicional, acero de alta resistencia, blindaje anti-soplete, blindaje antilanza térmica, hormigón de resistencia normal, hormigón de alta resistencia, hormigón de fibras, armaduras tradicionales, armaduras especiales, combinaciones de diversos materiales.
- *Según su composición:* marco de puerta, hoja de puerta, reja interior, pestillería, apertura motorizada, cerraduras, retardadores, sistema de alarma y sistema de bloqueo.
- *Según el grado de seguridad.*

✓ **Cerraduras de seguridad**

Las cerraduras y mecanismos de apertura y cierre son dispositivos que se componen de elementos maniobrables manualmente o mediante dispositivos eléctricos o electromecánicos. Esta función asegura el desplazamiento de uno o varios pestillos o elementos de cierre que se alojan o introducen en uno o varios cerraderos dispuestos para tal fin.

Aplicación. Las cerraduras y mecanismos de apertura y cierre de seguridad son, por una parte, elementos fundamentales del control de accesos y, por otra, elementos complementarios de otros sistemas de seguridad.

Este tipo de dispositivos de seguridad son los elementos más complejos de los medios técnicos pasivos y los que presentan mayor número de variables a la hora de estudiar una correcta adecuación para cada aplicación.

Parámetros de selección. Las consideraciones básicas a tener en cuenta en el planteamiento y selección de la cerradura son:

- Adecuación y utilización.
- Características del soporte.
- Grado de seguridad del dispositivo.
- Operatividad y función.
- Amaestramiento y jerarquización.
- Modelo y tipología.
- Conservación y mantenimiento.
- Relación coste/eficacia.

Conservación y mantenimiento. Debido a la importancia que tiene su funcionamiento, las cerraduras y mecanismos de seguridad precisan un correspondiente plan de conservación y mantenimiento que garantice las condiciones iniciales de seguridad, esto es, la fiabilidad de todos sus elementos (equipo y material, sujeción del equipo, limpieza y funcionamiento de apertura y cierre).

Especificaciones de las cerraduras para control de accesos. Las cerraduras para control de accesos, de acuerdo a su función y aplicaciones de seguridad, deberán cumplir todas o parte de las siguientes *especificaciones*:

- La apertura de la puerta tendrá corrección de maniobra para que, sin necesidad de hacer apertura manual de ella, podamos invertir la orden y cerrarla de nuevo, a través de: un sensor capacitivo, tarjeta codificada, mando a distancia temporizadamente o pomos de giro.

- El cierre de la puerta, una vez traspasada ésta, deberá realizarse de forma totalmente automática, mediante cierrapuertas exento de temporizaciones.
- El módulo de conjunto deberá ser antivibratorio, o sea, éste no deberá de seguir cargado por palancas o trinquetes retenidos por muelles, los cuales son fáciles de descargar por golpes, con lo que la seguridad del sistema se vería mermada.
- En caso de existir la señalización de apertura de puerta, su indicación al módulo de control debe partir del propio cierre.



✓ **Sistemas de amaestramiento y jerarquización de llaves.**

El amaestramiento es un sistema integrado de cierre, en el que una serie de llaves (maestras) abren más de un bombillo, independientemente de que cada bombillo tenga su propia llave. El amaestramiento es el sistema que permite establecer

un adecuado control de las cerraduras y accesos, así como una reducción del número de llaves a manejar.

Aplicación. El plan de cierre de amaestramiento y jerarquización es el establecido para que cada puerta (bombillo) sea abierta sólo por las llaves determinadas y por las personas que se consideren adecuadas.

Tipos. La tipología del amaestramiento permite su clasificación general en:

- **Amaestramiento sencillo:** cada punto del plan de cierre es abierto por su propia llave y por otra, maestra, que abre todos los puntos del plan de cierre.
- **Amaestramiento en grupos:** formado por grupos independientes, cada uno con llave maestra, y una llave, gran maestra, que abre todos los puntos del plan de cierre.
- **Amaestramiento en acceso principal:** cada llave abre su correspondiente punto del plan de cierre, y además abre los puntos de servicios comunes.
- **Amaestramiento cruzado:** una llave maestra de un grupo puede también abrir uno o varios bombillos de grupos diferentes. Es el sistema jerarquizado más complejo, dispone de llaves que sólo abren un punto, llaves sub-maestras, llaves maestras y llave gran maestra.

El elemento de las cerraduras que permite llevar a cabo el sistema de amaestramiento, es el cilindro que acciona la cerradura.

Ventajas que aporta el amaestramiento:

- **Servicio:** evita un número elevado de llaves a los directivos y responsables de Seguridad, mantenimiento, limpieza, etc.
- **Seguridad:** tanto en los accesos como en caso de evacuación y control de todos los accesos por el personal de Seguridad (podrán abrir cualquier puerta en cualquier momento).
- **Control de accesos:** ordenación y adecuado control mediante el establecimiento del plan de cierre.

- **Economía:** mayor eficacia de las cerraduras al estar controlada la reproducción de llaves. Todo cilindro de seguridad no necesita especial mantenimiento, debiendo soportar más de 500.000 ciclos como vida media.

✓ **Torniquetes y portillos**

Los torniquetes se definen como un dispositivo en forma de cruz con brazos iguales, que gira sobre un eje y que controla el acceso mediante el paso de las personas una a una.

Aplicación. Los torniquetes son de aplicación para áreas de acceso o salida de público y personal empleado. Además de cumplir funciones de control de accesos, pueden incorporar control horario, control de ocupación y control de visitantes a una determinada instalación. Todo ello de formas autónomas o integradas en el sistema central de control de accesos de la instalación.

La **tipología** de equipos para control de accesos de personas, existentes en el mercado bajo la denominación genérica de torniquetes, así como las especificaciones básicas de aplicación, se puede establecer:

- **Torniquetes trípode-horizontales.** Son los que afectan el control de paso mediante la rotación de un trípode que es empujado por el usuario y a cada vuelta permite el paso de una persona, quedando siempre uno de los brazos del trípode en posición de cierre. Pueden desarrollar diferentes funciones según aplicaciones específicas.
- **Molinetes giratorios verticales.** Tienen un sistema de funcionamiento idéntico al de los torniquetes horizontales, basando su diferencia en su concepción como molinete giratorio de alta o baja altura, en los que las palas u obstáculos son desplazados por el propio usuario.
- **Portillos.** Están basados, a diferencia de los torniquetes, en la filosofía de pasillo libre, o sea, sin obstáculos, de forma que al liberar el paso el espacio del pasillo quede libre sin necesidad de empujar ningún elemento, lo que facilita el tráfico en instalaciones de gran afluencia de público.

Estos sistemas son para instalar en lugares con vigilancia (humana o electrónica) ya que si son utilizados incorrectamente pueden dar señal de alarma y puede producirse el bloqueo del sistema.

✓ **Barreras de control de vehículos**

Las barreras de control de vehículos son los dispositivos de protección pasiva que, formando una barrera física o mediante barras o hileras de elementos, se disponen para el control de accesos de vehículos o ante intentos de intrusión no autorizados. Igualmente, según sea su diseño e implantación, las barreras permiten ser utilizadas como un sistema de seguridad disuasorio e, incluso, como elementos de protección ante la agresión o paso forzado.

Aplicación. Las barreras de control de vehículos son de aplicación para grandes formatos comerciales.

La **tipología** de las barreras de control de vehículos existentes, según su función, se clasifican básicamente en:

- *Según su tipología general:* fijas/ancladas, basculantes, ascendentes y extensibles.
- *Según su operatividad:* manual, semiautomática, automática, automática manual.

Barreras automáticas. Por su mayor aplicación en áreas comerciales, se tratan a continuación algunos de los aspectos más significativos de las barreras automáticas diseñadas para control de accesos de vehículos, a las que se puede dotar de un determinado grado de seguridad en función de su aplicación o necesidad.

Las barreras automáticas han de ser proyectadas para ofrecer seguridad y acceso regulado a zonas controladas y han de satisfacer criterios de máxima funcionalidad, insonorización, absoluta fiabilidad en cualquier condición de uso y precisos criterios de seguridad.

La dotación y equipamiento de las barreras automáticas estarán directamente relacionados con el programa de funciones y necesidades que se deseen cubrir. Las especificaciones y componentes que básicamente han de configurar en dicho equipamiento, son:

- Dimensiones de acceso a controlar.
- Ubicación del grupo conjunto de mecanismos.
- Elementos de seguridad (obstáculo escamoteable empotrado en el suelo, grada articulada, faldón rígido o flexible, etc.).
- Sistema de apertura de la barrera (por detector de presencia, tarjeta, operador, etc.).
- Material y dimensiones.
- Tiempo de maniobra.
- Sistema de alimentación.
- Acabado y conservación.

3.1.2 PROTECCIÓN CONTRA HURTO, ROBO Y ATRACO

La protección contra hurto, robo y atraco, dentro de los términos generales de disposición de los elementos técnicos de seguridad pasiva, implica la implantación de los medios de prevención y protección necesarios para contrarrestar los riesgos y amenazas por sustracción de bienes.



Entre los principales materiales y equipos de seguridad pasiva para protección contra el hurto, robo y atraco, de aplicación a los establecimientos comerciales, cabe destacar:

- **Las mamparas y tabiques**, de especial protección para la compartimentación de áreas interiores de seguridad.
- **Los cerramientos y vallados, alambrados o enrejados**, para protección de áreas externas o perimetrales.
- **Los cierres y persianas de seguridad**, para escaparates, accesos y áreas de almacenes.
- **Las carcasas antihurto**, para protección de los artículos y mercancías en venta.

Son de aplicación complementaria los elementos y sistemas de control de accesos y protección ante la intrusión.

✓ **Mamparas y tabiques**

Las mamparas y tabiques son elementos arquitectónicos básicos de separación. Su empleo como pantallas de seguridad de interiores para protección ante la intrusión requiere un estudio previo para la adecuada adaptación a cada caso y circunstancia en función de las especiales implicaciones de seguridad.

Aplicación. En el mercado específico de la seguridad, existen modelos fabricados especialmente con dicha función y con distintos grados de seguridad. También existe la posibilidad de emplear materiales con condiciones especiales de seguridad en sistemas tradicionales de mamparas y tabiques, consiguiendo las condiciones de seguridad requeridas en cada caso.

La **tipología** de las mamparas y tabiques de seguridad que se puede establecer, de acuerdo a su función, es la siguiente:

- *Según la forma de montaje:* elementos fijos y elementos practicables.
- *Según el material en tabiques:* ladrillos, yeso/escayola, yeso/cartón, hormigones, fibrocemento, maderas, materiales sintéticos, materiales metálicos y combinaciones especiales.

- *Según la clase de construcción:* tradicional, industrializada y prefabricada.
- *Según el grado de seguridad:* resistencia al ataque con elementos manuales, con equipos mecánicos y con proyectiles ligeros.

De acuerdo a los parámetros y objetivos de seguridad específicos de cada instalación, con el estudio de la adecuada combinación y equilibrio de la diferente tipología de mamparas y tabiques, se plantearán las diferentes soluciones.

✓ **Cerramientos y vallados**

Son medios de protección perimetral que delimitan el área de propiedad y/o área de seguridad o recintos de riesgo especial para impedir, restringir o retrasar el intento de intrusión o la fuga desde el interior y dificultar la aproximación a locales o puntos vitales de la instalación.

Para conseguir los objetivos anteriores, los medios pasivos de protección perimetral a aplicar pueden ser: empalizados, enrejados y alambradas.

Aplicación. Cada uno de los tipos de cerramientos y vallados será de aplicación de acuerdo a las necesidades específicas de seguridad y al establecimiento de sus objetivos de protección perimetral.

Para la definición de los medios pasivos a implantar, será de especial importancia tener en cuenta los posibles métodos de intrusión a los recintos protegidos.

Debido a la vulnerabilidad, en general, de los medios de protección perimetral ante la variedad y contundencia de los posibles métodos de intrusión, los medios pasivos deberán ser complementados, según los casos y circunstancias, con medios activos y/o humanos que nos puedan proporcionar la adecuada e inmediata información ante cualquier intento de intrusión.

Los cerramientos y vallados. Son elementos de cerramientos perimetrales exteriores, que se utilizan con o sin especiales condiciones de protección. **Se clasifican** en:

- *Según su tipología:* alambradas, empalizadas y enrejados.
- *Según el material empleado:* aceros, aleaciones ligeras, hormigones y maderas.
- *Según los medios de ataque:* simples, compuestos, complejos y sofisticados.
- *Según el grado de seguridad:* paso por debajo, a través, por encima y por destrucción.

La determinación del modelo de valla a instalar se definirá en función de los criterios siguientes:

- Riesgos analizados.
- Grado de seguridad a obtener.
- Cálculos de carácter técnico: naturaleza del terreno, vientos dominantes, temperaturas mínimas y máximas, sismología, sistema de seguridad en el que se integra la valla, etc.

✓ **Cierres y persianas**

Los cierres y persianas son elementos tradicionales de la arquitectura y la construcción, a los que se podrá dotar de funciones específicas de seguridad para protección ante la intrusión, en función de las características específicas de su construcción.



Aplicación. Su aplicación será tanto en interiores, escaparates de tiendas y accesos como para la protección exterior en el mismo perímetro de un gran formato comercial. **Se clasifican** en:

- *Según su tipología:* plegables, extensibles, enrollables, abatibles y deslizantes.

- *Según el material empleado:* aceros normales, aceros especiales, aleaciones ligeras, materiales sintéticos, maderas y combinaciones de varios de ellos.
- *Según su accionamiento:* manual, mecánico, electromecánico y neumático.
- *Según el grado de seguridad:* ataque con medios manuales, con equipos mecánicos y con proyectiles ligeros.

Es de destacar la gran importancia que tiene que los cierres y persianas estén diseñados y fabricados realmente como elementos de protección, así como lo fundamental que resulta para su función de seguridad que estén recibidos o anclados adecuadamente en los huecos disponibles.

✓ **Carcasas para protección antihurto**

Las carcasas para protección antihurto son cajas transparentes que contienen en su interior el producto a la venta y que están dotadas con un dispositivo electrónico que avisa cuando se intenta traspasar una antena de detección sin que este dispositivo electrónico esté desactivado. Al realizarse la venta del artículo, se procede a su retirada, el producto queda liberado y puede atravesar la antena de detección sin incidentes. Este tipo de carcasas son reutilizables en su totalidad. Las carcasas de protección antihurto combinan la protección pasiva con la activa.

La protección pasiva contra el hurto mediante este tipo de sistemas de protección ha de considerar dos grandes parámetros: por un lado, la imagen de la organización y de la marca del producto en exposición; y por otro, la rentabilidad de utilización de este tipo de protección con respecto al valor del producto protegido y al incremento de la cuenta por pérdida desconocida.

3.1.3 PROTECCIÓN ANTE LA AGRESIÓN

La protección ante la agresión puede ser definida de una manera general como los obstáculos implantados y organizados con el objetivo de evitar o minimizar las consecuencias de las agresiones a personas, vehículos y objetos.

Entre los principales equipos de seguridad pasiva para la protección ante la agresión, de aplicación a los establecimientos comerciales, se encuentran:

Los mostradores blindados, para zonas especiales.

Los acristalamientos de seguridad, para áreas de caja central o zonas de especial protección.

Las láminas de protección, para vidrios en escaparates.

La protección ante pintadas y *graffitis*, para protección de superficies.

• **Cabinas y mostradores blindados**

Las cabinas y mostradores blindados son elementos de protección normalmente cerrados que, en función de su situación y aplicación, incorporan mostradores normales o especiales, fijos o móviles, y que están constituidos por mamparas o paneles transparentes u opacos, que configuran una aplicación contra agresiones.

Aplicación. Debido a sus múltiples y diferentes aplicaciones, así como a la variedad de materiales de blindaje posibles de utilizar, las cabinas y mostradores de seguridad requieren un planteamiento específico desde su definición y diseño hasta su implantación. Los parámetros mínimos a definir serán:

- El área de seguridad.
- Los riesgos a que estarán sometidos.
- El grado de seguridad requerido.
- El tipo y características funcionales.
- Las características técnicas de construcción.

Las cabinas y mostradores de seguridad **se clasifican** en:

- *Según su tipología*: protección de áreas, cabinas de protección y garitas de vigilancia.

- *Según su emplazamiento:* áreas interiores y exteriores.
- *Según su composición:* estructura, elementos fijos y practicables (transparentes, translúcidos y opacos) y elementos complementarios (pasadocumentos, pasapaquetes, comunicaciones, sistema de alarma, ventilación, climatización, etc.).
- *Según su fabricación:* prefabricada, modular, industrializada y específica.
- *Según su aplicación:* protección, vigilancia y control.
- *Según el grado de seguridad:* antiintrusión, antivandalismo, antimotín y antibala.

Las cabinas y mostradores requieren normalmente de equipamiento de seguridad, y éste se define como el conjunto de equipos especiales o complementarios que, dispuestos en mostradores o empanelados, favorecen el funcionamiento y operatividad de los locales o recintos protegidos ante posibles agresiones. Este equipamiento especial podrá ser:

- *Según su utilización:* pasadocumentos (bandeja fija o móvil), pasapaquetes (en esclusa, cajón móvil y carro en esclusa) y troneras.
- *Según su funcionamiento:* dispositivo fijo o móvil (mecanismo manual o motorizado).
- *Según sus materiales:* aceros normales o especiales, aleaciones ligeras, vidrios, sintéticos y combinación de varios materiales.
- *Según su emplazamiento:* en el interior o exterior.
- *Según su grado de seguridad:* antiatraco, antiagresión y antibala.

Todos los elementos que conformen el equipamiento especial de cabinas y mostradores, estarán adaptados al grado de seguridad de éstos.



- **Acristalamientos de seguridad**

Los blindajes transparentes o translúcidos son pantallas laminares, destinadas a ofrecer una protección contra el ataque mediante proyectiles ligeros u objetos contundentes, que están formados por una o varias láminas de material de igual o diferente resistencia mecánica.

Aplicación. En las áreas de caja central y otros recintos que requieran especial protección propia de los grandes formatos comerciales, puede ser necesaria la instalación de materiales blindados que, por la propia actividad u operatividad, requerirán ser transparentes o translúcidos.

Estas pantallas laminares que dan lugar a los acristalamientos de seguridad, pueden ser:

- *Productos vítreos:* vidrios de seguridad de aplicación generalizada en blindajes.

- *Cristales de policarbonato:* a igualdad de espesor que los vidrios, proporcionan una mayor resistencia a los impactos.
- *Acristalamientos mixtos vidrio y policarbonato:* de empleo, sobre todo, en aplicaciones curvas para vidrios blindados y exigencias de espesor reducido.
- *Cristales acrílicos:* su resistencia al impacto es menor que la que proporcionan los cristales de policarbonato o las láminas de vidrio, se deterioran con el paso del tiempo, pues les afectan los rayos ultravioletas.

• Láminas de protección

A efectos de incrementar la seguridad de los acristalamientos, fundamentalmente de los instalados en escaparates, se pueden emplear las láminas de protección para cristales que son materiales flexibles, generalmente adhesivos que, incorporados a los vidrios, se unen a ellos proporcionándoles distintos grados de resistencia frente a diversos agentes agresivos.

Aplicación. Las láminas de protección son de aplicación para los escaparates de las tiendas del interior del centro comercial.

Los diversos tipos existentes tienen, en general, las siguientes características comunes:

- Una o varias láminas fabricadas sobre soporte de poliéster transparente de diversos espesores que ofrecen una resistencia proporcional al mismo.
- Un adhesivo de base acrílica, sensible a la presión y reactivable con el agua y que posee poca adherencia inicial, lo que facilita su colocación.
- Un recubrimiento especial de la lámina transparente para conseguir propiedades especiales.

Las **funciones** de las láminas de protección consisten en: mantener unidos los fragmentos de un vidrio en caso de rotura, con lo cual se pueden evitar accidentes por proyección de los fragmentos o esquirlas en caso de explosión, resistir el ataque con

proyectiles o choque accidental y sujetar el acristalamiento, impidiendo de una manera eficaz (en función de los medios y del tiempo de duración del ataque) la apertura de un hueco para penetración de intrusos, evitar la propagación del fuego, evitar el robo, etc.

Algunos de los aspectos a tener en cuenta en la instalación de las láminas de protección, son:

- *El riesgo proviene del exterior del acristalamiento:* la lámina debe ser colocada en el interior del elemento a proteger.
- *El riesgo proviene del interior o exterior del acristalamiento:* la lámina debe colocarse por ambas caras del vidrio.

• Protección ante pintadas y *graffitis*

Las pinturas antigraffitis son recubrimientos especiales que protegen las superficies contra las agresiones gráficas convirtiéndolas en lavables y facilitando la limpieza de las mismas.

Aplicación. Las pinturas protectoras ante



pintadas y *graffitis* son de aplicación en los formatos comerciales que tienen áreas de ocio. Estas zonas, con frecuencia son agredidas por jóvenes que, arropados por lo que pretende ser una expresión cultural, deterioran y ensucian las instalaciones. Los *graffiteros* son en general jóvenes (menores de quince años) que, armados con gruesos rotuladores de colores o con *sprays*, pintan las paredes de las instalaciones para difundir sus mensajes o afianzar su presencia mediante su omnipresente firma.

Los *graffiteros* producen molestas pintadas que perjudican la imagen, deterioran las instalaciones comerciales y aumentan la sensación de inseguridad ciudadana.

Como medidas concretas para la protección de las instalaciones contra este tipo de agresiones, en los últimos años se han reforzado las medidas físicas de protección para fluorescentes, cristales de escaparates, cerraduras, así como pinturas especiales para evitar la adherencia de *graffitis* y pintadas en aquellas superficies susceptibles de ser su soporte.

3.1.4 PROTECCIÓN DE INFORMACIÓN Y VALORES

La protección de información y valores implica *la implantación de aquellos elementos o construcción de habitáculos que han de ofrecer un grado de seguridad para la protección de bienes, información y valores frente a la manifestación de diferentes riesgos.*

Entre los principales equipos y sistemas de seguridad pasiva para protección de la información y valores, de aplicación a los establecimientos comerciales, cabe destacar:

Las cajas fuertes, para custodia de valores y efectivo.

Los armarios de seguridad, para protección de información.

Las cámaras acorazadas y recintos protegidos, para conteo y protección del dinero en efectivo.

Los submostradores o cajas antiatraco, para áreas de cajeros.

Los cajeros automáticos, para atención al público.

La caja de tránsito, para autogestión del efectivo.

Armeros, para la custodia de armas.

Valijas de seguridad, para el transporte de la información y valores.

• Cajas fuertes y armarios de seguridad

Las cajas fuertes y armarios de seguridad constituyen el conjunto de defensas físicas que delimitan un recinto autónomo o espacio a proteger, de pequeño o gran volumen, accesible a través de una o varias puertas y cuyo grado de seguridad es homogéneo en todas y cada una de sus caras y elementos que constituyen el conjunto.

La **tipología** de cajas fuertes y armarios existentes, así como sus principales aplicaciones específicas, están recogidas en la siguiente clasificación general:



- *Según su utilización:* custodia de valores y efectivo, protección antiatraco, recaudación específica, protección de cajeros automáticos y protección de buzones.
- *Según su ubicación:* autónoma, anclada o empotrable.
- *Según su volumen útil:* menor de 50 litros, de 51 a 100 litros, de 101 a 200 litros, de 201 a 500 litros y mayor de 500 litros.
- *Según el grado de seguridad.*

El Reglamento de Seguridad Privada y otra normativa al respecto determinan las características y medidas de protección de las cajas fuertes.

La fabricación de cajas fuertes de aplicación a la protección de información y valores no está sujeta a normas técnicas. Su diseño y construcción es de carácter libre y son los ensayos de calificación los que determinan su grado de seguridad y condiciones específicas de calidad.

Armarios ignífugos. Un armario ignífugo es un armario de seguridad dotado de las características necesarias, en cuanto a su fabricación, para garantizar la inalterabilidad de su contenido, bienes y bancos de datos, contra los efectos del fuego y elevadas temperaturas.

Su tipología y aplicaciones específicas básicamente son las mismas que para las cajas fuertes.

Los soportes de información representan un valor incalculable para las entidades, para garantizar su protección ante la manifestación de los diferentes riesgos, los armarios de seguridad e ignífugos son el medio pasivo adecuado para su preservación, proporcionando protección contra robo, fuego, gases inflamables, humedades y campos magnéticos.

• **Cámaras acorazadas**

Las cámaras acorazadas son recintos de seguridad cerrados, formados por un conjunto de defensas físicas integradas por muros y/o paneles y forjados acorazados, que delimitan el espacio a proteger y que pueden ser accesibles por una o varias aberturas controladas por puertas y trampones acorazados. A dichos recintos se les dotará de protecciones electrónicas complementarias, como medios de alarma, vigilancia y control. Igualmente, es aconsejable que la cámara acorazada esté dotada de una antecámara en la que pueda penetrar un vehículo blindado para la protección de la entrega/retirada de efectivo.

La **tipología** de las cámaras acorazadas, así como sus principales aplicaciones específicas, están recogidas en la siguiente clasificación general, realizada en función de:

- *Según su función o utilización:* cámara de valores, de efectivo y para usos especiales.
- *Según su ubicación:* edificio o local propio o único y edificio o local compartido.
- *Según su localización:* planta bajo rasante, nivel de calle o a nivel de piso.

- *Según su construcción:* tradicional, industrializada o prefabricada.
- *Según su grado de seguridad* relacionado con el tipo de equipo de ataque posible de utilizar y el tiempo que debe resistir al mismo.

El Reglamento de Seguridad Privada y otra normativa al respecto determinan las características y medidas de protección de las cámaras acorazadas.

Los criterios más importantes que se deben observar en la definición de la composición y equipamiento de la cámara acorazada o en la decisión de simplemente instalar un recinto protegido son: *parámetros de diseño, componentes del recinto y procedimiento de construcción.*

Parámetros de diseño

- Situación de los locales, comprobando la posible existencia de pozos, canalizaciones, túneles, etc.
- Posición de los cerramientos respecto al tráfico, edificios anejos, patios, solares o calles, etc.
- Organización y distribución esquemática de las áreas de actividad.
- Posible ubicación prevista para la cámara dentro del edificio, planta, área, etc.
- Características de la estructura, forjados, muros, cimentación, etc.
- Situación del nivel freático y características del terreno natural.
- Ubicación de los sistemas de aire acondicionado, calefacción y ventilación de locales adyacentes.
- Comprobación del tipo de dimensiones de las vías de circulación y accesos al edificio y cámara.
- Situación y distribución de las instalaciones de fontanería y electricidad del local y edificio.
- Comprobación de los condicionamientos de tipo arquitectónico que posee el edificio.

- Recopilación de los datos estadísticos sobre riesgos o desastres naturales ocurridos.
- Comprobación de implicaciones derivadas de la legislación municipal, comunitaria y gubernativa.
- Determinación y definición del tipo de cámara acorazada, características y dimensiones.
- Evaluación de los subterráneos de la zona afectada por el edificio o cámara acorazada.

Componentes del recinto. Posible equipamiento

- Puerta principal.
- Puerta de emergencia.
- Muros de cerramiento.
- Muros de ronda.
- Ventilación.
- Detección y alarma de intrusión.
- Vigilancia por CCTV.
- Detección y alarma de incendios.
- Amplia antecámara con acceso para furgón blindado.
- Extinción de incendios.
- Climatización e iluminación.
- Comunicaciones.
- Motorización de puertas.
- Retardos o enclavamiento de accesos.



- Conexión de buzones.
- Sistemas de emergencia.
- Sistemas neumáticos.

Procedimiento de construcción

- Sistema tradicional. Hormigón especialmente armado y, eventualmente, planchas de acero.
- Sistemas prefabricados. A base de paneles prefabricados especiales. Estos sistemas han alcanzado un grado de seguridad importante con espesores reducidos, con grandes ventajas en todas las aplicaciones.

• Submostradores

Las cajas fuertes antiatraco, denominadas submostradores, para áreas de cajeros, son cofres de seguridad con cajones para operaciones con efectivo y departamento para custodia que está temporizado.

Aplicación. Los submostradores son de aplicación en zona de cajeros.

La **composición mínima**, en cuanto a compartimentación, de los submostradores, habitualmente suele ser: cajón de operaciones; área escamoteable; y área de apertura retardada.

Las **características básicas** que deben cumplir los submostradores en cuanto a su fabricación son:

- Facilidad de activación de la temporización.
- Posibilidad de variación de la temporización mediante cerradura mecánica de tiempo o sistema electrónico programable.
- Temporización sin clave ni combinación.

- Protección bajo llave de control de temporización, incluida en el cajón o área escamoteable o en control remoto.
- Posibilidad de transmitir alarma.
- Señal óptica intermitente acoplada exterior al submostrador.
- Cajón escamoteable no desmontable fácilmente mediante tirón.

Bajo estas características básicas de diseño, se realizarán las especificaciones de acuerdo a las necesidades concretas de la instalación. Se tendrá en cuenta, igualmente, el grado de seguridad requerido.

• **Cajeros automáticos**

Los cajeros automáticos, que pueden estar distribuidos en los grandes formatos comerciales, son sistemas automáticos completos de servicios bancarios en los que los usuarios pueden realizar un gran número de operaciones y obtener dinero en efectivo.

La introducción de cajeros automáticos con la finalidad de mejorar y ampliar los servicios a sus clientes se ha prodigado con notoriedad en los últimos años.

Esta evolución o proceso se ha caracterizado por las respuestas dadas por la Dirección de los propios establecimientos comerciales, junto con las entidades bancarias, en la instalación de cajeros; debido a la demanda social, la propia competitividad del mercado, las necesidades de protección de los equipos y las exigencias que en materia de seguridad ha venido estableciendo la Administración del Estado.

Los cajeros automáticos están considerados, en parte, como las agencias bancarias del futuro por las prestaciones que proporcionan actualmente y las que se irán incorporando sucesivamente. Entre ellas cabe destacar: disminución de los tiempos de espera en las sucursales bancarias para realizar operaciones simples o bien para realizar consultas; permite ingresar y dispensar efectivo; permite conocer en tiempo real los saldos y movimientos y actualizarlos, etc.

Las exigencias en materia de seguridad que afectan a los cajeros automáticos las podemos desglosar en:

- Intrínsecas de los propios equipos.
- Exigidas por la normativa de la seguridad privada vigente.

Entre las medidas de seguridad intrínsecas a los propios equipos, podemos destacar:

- Cabinas de frontal indismontable de acero con sistemas antipalanca.
- Sistema de protección integral, lógico y físico del efectivo.
- Sistema de cierre independiente en el módulo ingresador/dispensador.
- Sistema de apertura retardada.
- Llave electrónica.
- Sistema de alarma silenciosa.

Para completar estas medidas de seguridad intrínsecas, el Reglamento de Seguridad Privada y otra normativa al respecto, concretan determinados aspectos en materia de medidas de seguridad.

• **Cajas de tránsito**

El sistema de caja de tránsito consiste en una caja fuerte con dos puertas (situadas una hacia el exterior y otra hacia el interior de la instalación) que cuenta con dispositivos internos de autogestión inteligente del efectivo.

Aplicación. La posible adopción de este sistema está dirigido a la mejora de los distintos componentes que integran la gestión del efectivo en las empresas y entidades que manejen gran cantidad del mismo, aumentando los niveles de seguridad, ya que elimina el riesgo en la entrega/recogida, diversifica el efectivo y aumenta los controles operativos mejorando los niveles de productividad y de gestión.

Ello permite que las recogidas y entregas de efectivo no requieran de contacto directo entre los empleados y la empresa encargada del transporte, lo que supone una doble ventaja: se liberan los horarios y no se accede al interior de las instalaciones.

El sistema de caja de tránsito consiste básicamente en el trazado de un bucle operativo cuya sistemática se podría resumir:

- El *host* del establecimiento comercial solicita al de la empresa de seguridad la retirada o entrega del efectivo necesario.
- Esta petición se introduce en las terminales portátiles que acompañan a las sacas del efectivo, que han sido selladas mediante precintos microprocesados.
- El vehículo de transporte recoge o lleva la remesa solicitada a su destino y conecta su terminal con la caja de tránsito en su parte exterior, para introducirse en su base de datos y modificarla con arreglo al contenido de la saca y las operaciones programadas y autorizadas.
- Cuando se necesite efectivo se abrirá la caja por su parte interior, siguiendo las operaciones programadas a tal efecto.

Las exigencias que en materia de seguridad afecta a las cajas de tránsito se pueden desglosar en:

- Intrínsecas de los propios equipos.
- Exigidas por la normativa de seguridad privada vigente.

Entre las medidas de seguridad intrínsecas a los propios equipos, podemos destacar:

- Alarmas de coacción.
- Alarmas y bloqueos por operaciones no autorizadas.
- Funciones de identificación de usuarios.
- Uso combinado de llaves físicas y electrónicas.
- Cerraduras borrables y cambiables.

- Conmutación y gestión de apertura de puertas.
- Sistema de retardo.

• **Armeros**

Los armeros son armarios de seguridad exigidos para la custodia de las armas.

De acuerdo a las Ordenes Ministeriales por las que se concretan determinados aspectos en materia de empresas y medidas de seguridad, dando cumplimiento al Reglamento de Seguridad Privada, los lugares donde se preste servicio de vigilantes de seguridad con armas deberán disponer de armeros que reúnan una serie de medidas de seguridad tanto pasivas como activas.

Las características técnicas de dichas medidas vendrán recogidas en el Plan de Protección de la Instalación.

En cuanto a las normas generales sobre "Armeros", habrá de tenerse en cuenta, igualmente, lo establecido en el Reglamento de Seguridad Privada.

• **Valijas de seguridad**

La protección de la información y valores implica, por un lado, el dispositivo físico de transporte para control de la información y valores generados en la actividad comercial y, por otro, la implantación y organización del servicio de transporte.

Las valijas son sacas o portadocumentos provistos de candado u otros dispositivos de cierre (precintos de seguridad), que se utilizan para transportar documentos reservados, de carácter confidencial o fondos y valores.

Estas valijas pueden contar con otros elementos adicionales que hacen que sea inútil cualquier intento de manipulación externa, ya que incorporan dispositivos internos que destruyen el contenido (explosión, tinta, cambio de color, etc.) por lo que se procede a la inutilización del valor del contenido.

Para la determinación de la necesidad de utilización de este tipo de medida de seguridad, será necesario definir:

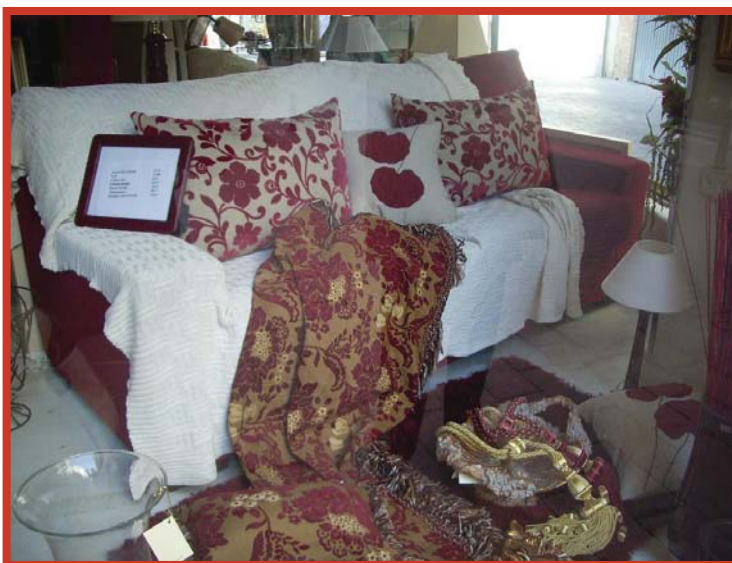
- Organización esquemática de las áreas de actividad donde se maneje información confidencial.
- Determinación de los niveles de confidencialidad de los documentos.
- Determinación de las personas implicadas en la clasificación, manipulación y recepción y destino de la documentación confidencial.
- Determinación de frecuencias, rutas, destinos y tipos de valijas a emplear.

El transporte de fondos y valores. La legislación establece que “Los establecimientos comerciales efectuarán el transporte de monedas, billetes, títulos-valores y objetos preciosos; a través de las empresas de seguridad autorizadas para tal actividad”.

Aplicación. Para el desarrollo de esta actividad es aconsejable que el establecimiento comercial cuente con una zona de carga y descarga, comunicada con el exterior con un sistema de puertas esclusas con dispositivo de apertura desde su interior. Los muros y puertas de dicha zona, deberán cumplir las características de blindaje, en cuanto a su configuración y materiales, indicados en este capítulo para los muros, puertas de seguridad y acristalamientos de seguridad.

3.1.5 PROTECCIÓN PASIVA CONTRA INCENDIOS

La protección pasiva contra incendios es el conjunto de medios, elementos y características físicas que ha de reunir el edificio o recinto a proteger, tendentes a evitar las pérdidas y daños producidos por el fuego, impidiendo que éste se propague y ponga en



peligro la vida de las personas y bienes.

La aplicación de medios técnicos pasivos y elementos constructivos apropiados a la protección pasiva, debe perseguir los **objetivos** siguientes:

- Asegurar la estabilidad del edificio.
- Compartimentar y sectorizar adecuadamente para impedir la propagación del fuego.
- Asegurar la evacuación de las personas.
- Reducir los efectos del fuego.
- Facilitar los trabajos de extinción.

Para el estudio y definición de los diferentes materiales, productos y equipos de aplicación a la protección pasiva contra incendios en establecimientos comerciales, planteamos éste como un gran sistema del que formen o pueden formar parte todos o algunos de los materiales, productos y equipos correspondientes a:

Protección estructural.

Compartimentación.

Evacuación de humos.

• Protección estructural

Lo constituye el conjunto de medios de protección que asegura la estabilidad de las diferentes partes estructurales, cerramientos y decoración del edificio frente a un incendio y los posibles daños causados por la acción del fuego.

Las medidas y medios que conforman el subsistema de protección estructural, básicamente son:

- Medidas constructivas.
- Materiales de construcción.

- Elementos constructivos.
- Revestimientos ignífugos. Ignifugación de mobiliario y elementos decorativos.
- Vidrios cortafuego.

Medidas constructivas. Las medidas de tipo constructivo necesarias a implantar, al menos, deben ser:

- *Protección de la estructura.* Las exigencias del comportamiento ante el fuego de un elemento constructivo se definen por el tiempo que dicho elemento mantiene:

La estabilidad o capacidad portante.

La ausencia de emisión de gases inflamables por la cara no expuesta.

La estanquidad al paso de llamas o gases calientes.

La resistencia térmica suficiente para impedir que se produzcan, en la cara no expuesta, temperaturas superiores a las citadas en la norma tecnológica al respecto.

- *Limitación de la combustibilidad de los materiales de revestimiento, acabado y decoración.* Bien eligiendo los de naturaleza no combustible ni tóxica por combustión, o realizando un tratamiento sobre los mismos de "ignifugación" que produzca igual efecto.

- *Compartimentación de los recintos.* Basada en un diseño que permita la operatividad funcional pero a la vez impida la propagación del fuego de unos recintos a otros, con el adecuado tratamiento de los huecos existentes, tanto para paso de personas como de canalizaciones.

- *Diseño y tratamiento de las vías de evacuación.* De tal modo que éstas no resulten dañadas por los efectos del incendio (calor, humo y llamas).

- *Control de humos.* Con el fin de que éstos no causen problemas de toxicidad ni afecten a la visibilidad, ni lleguen a producir sobrepresiones causantes de la contaminación de otros recintos.

Como medida anexa a las constructivas deberá tenerse en cuenta la señalización: que permita identificar rápida y fácilmente las vías de escape, la situación de cada persona en relación con el edificio (es decir, la orientación dentro de la distribución interior del mismo) y el nivel de riesgo relativo de cada recinto.

Materiales de construcción. Declarado un incendio, el proceso constructivo y de diseño del edificio actúa en el control del incendio mediante la adecuación del comportamiento ante el fuego de los materiales constructivos, muy especialmente de aquéllos que con mayor probabilidad puedan entrar en combustión:

- Todos los materiales de revestimiento o acabado superficial, por cuanto el foco de ignición o calor es aleatorio, indiscriminado y no identificable *a priori*.
- Todos aquellos materiales que, sin ser vistos o de acabado superficial, tengan mayor probabilidad de entrar en combustión por su proximidad a un foco potencial, pero identificado, de calor o llama.

El cumplimiento de las limitaciones reglamentarias establecidas para los materiales, debe estar fundado en un parte del técnico que actúe en el proceso de edificación, en certificados de ensayos y clasificación emitidos por laboratorio oficialmente acreditado para este fin.

Elementos constructivos. La acción del fuego impone la necesidad de que los elementos estructurales aporten una determinada resistencia al mismo, evaluada en términos de tiempo durante el cual mantienen su función estructural propia y la de compartimentación, caso que la sectorización del edificio le asigne tal función, así como la de ausencia de emisión de gases inflamables.

Los elementos constructivos fundamentales a tener en cuenta, en cuanto a su grado de resistencia al fuego, son: fachadas, cubiertas, puertas, falsos techos y cámaras, conductos y espacios ocultos.

Revestimientos ignífugos. Ignifugación de mobiliario y elementos decorativos. La ignifugación es el tratamiento que se da a los materiales para mejorar su "clase", es decir, su clasificación a efectos de mejorar su reacción al fuego. Por lo que la acción de los productos incorporados al material mediante dicho tratamiento, se puede traducir en una inhibición de la inflamabilidad del material base, pero no actúa sobre su combustibilidad.

Los revestimientos y elementos ignífugos pueden ser:

- *Intumescentes:* por intumescencia se entiende el efecto de aumento de volumen o expansión de una sustancia bajo la acción del calor, creando una capa espumosa de materiales carbonizados que sirve de aislante en el proceso de combustión. Su utilización más difundida es en forma de pinturas y barnices aplicables sobre estructuras y recubrimientos de madera o metal, aunque también se encuentra disponible en forma de pasta, masilla, mortero, tableros, etc., permitiendo su utilización en aplicaciones muy diversas.
- *Aislantes:* el aislamiento se consigue mediante la aplicación de productos tales como morteros ignífugos (de cemento, yeso, perlita, vermiculita, amianto, lana de roca, fibras cerámicas, etc.), productos selladores, placas aislantes, etc. Un aspecto muy importante de los tratamientos de ignifugación es la durabilidad del tratamiento ante acciones exteriores. Será muy importante exigir al suministrador certificado a este respecto, dado que la responsabilidad que el material mantenga a lo largo del tiempo y la clase de reacción al fuego que le sea exigible recae en el propietario o titular del edificio.

Vidrios cortafuego. Como parte de la protección del edificio, los vidrios tienen la misma importancia que el resto de materiales que deben asegurar la estabilidad del edificio. Si los vidrios no presentan un tratamiento adecuado, iniciado el incendio, se

romperán permitiendo la entrada de aire fresco y, por tanto, de oxígeno, activando la combustión y creciendo el fuego en intensidad.

Los vidrios cortafuego gracias a su función divisoria, que mantienen durante un determinado periodo de tiempo, impiden la propagación del fuego y humos.

Según su función, se clasifican en:

- *Parallamas*. Mantiene su integridad.
- *Cortafuego*. Mantiene su integridad y aislamiento térmico.
- *Resistentes al fuego*. Mantiene su estabilidad, estanquidad, no emisión de gases inflamables y aislamiento térmico.

• **Compartimentación**

Lo constituyen el conjunto de dispositivos dirigidos a separar espacios, denominados sectores de incendio, por medio de elementos resistentes al fuego, para evitar la propagación de un incendio.

Los medios de compartimentación que conforman este subsistema, principalmente son:

- Puertas cortafuego.
- Muros y paneles para compartimentación.
- Compuertas cortafuego.
- Medios complementarios.

Puertas cortafuego. Son las diseñadas para resistir durante un determinado período de tiempo su exposición directa al fuego, sin alterar ninguna de sus propiedades.

La experiencia sobre incendios reales y las correspondientes estadísticas demuestran la decisiva influencia de las puertas en la propagación de incendios. Un

elevado porcentaje encuentra su difusión a través del más evidente “punto débil”, de aquellos parámetros que tienen la función de contener el fuego: los huecos de paso y las puertas.

La respuesta de una puerta ante el fuego, se establece conforme a dos criterios:

- Su capacidad para contener el incendio.
- Su capacidad como barrera ante el paso de humos.

Donde el cumplimiento del primer criterio durante el tiempo exigible, no implica necesariamente el cumplimiento del segundo. Una puerta resistente al fuego necesita determinadas características adicionales para poder limitar el paso de humos, que generalmente consisten en elementos que cierran el paso del mismo a través de su perímetro.

La capacidad para contener el incendio, a su vez, se gradúa en dos niveles:

- Mantenimiento de su estabilidad mecánica, de estanquidad al paso de llama y ausencia de emisión de gases inflamables en la cara no expuesta (puerta PF “parallamas”, durante el tiempo que mantenga tales condiciones).
- Mantenimiento del aislamiento térmico, además de las condiciones anteriores, de forma que la temperatura media en la cara no expuesta, no supere los 140 °C, ni ninguno de sus puntos supere los 180 °C.

Los dos objetivos primarios de las puertas cortafuegos son proteger las zonas anexas y controlar el fuego durante el tiempo para el que están fabricadas.

Algunas de las características a tener en cuenta en cuanto a su aplicación son:

- Su posición debe ser normalmente cerrada, o bien su cierre comandado por medios electromecánicos.
- Deben poder abrirse con facilidad.
- El sentido de apertura debe coincidir con el de la evacuación.

- Las puertas RF que hayan de ser utilizadas como vías de evacuación deben ser equipadas con dispositivos de apertura antipánico.
- Las puertas a instalar estarán debidamente certificadas, de acuerdo a normas UNE, por laboratorio de ensayo homologado.



Muros y paneles para compartimentación. Son los muros y paneles diseñados para cortar el paso al fuego en caso de incendio.

En caso de incendio, el muro cortafuego o panel deberá mantener su:

- Aislamiento térmico.
- Estanquidad a las llamas.
- Estabilidad.
- Resistencia característica (para los muros de carga).

El tiempo máximo en que se cumplen estos requisitos simultáneamente da la clasificación a la resistencia del muro o panel.

Compuertas cortafuego. Están formadas, en general, por una caja intercalada en los conductos de ventilación a la altura de los forjados del piso o muros cortafuego de sectores de incendio diferentes. Esta caja contiene un dispositivo de cierre (compuerta) que actúa, en caso de incendio, automáticamente, mediante fusible o mando electromagnético operado por un detector de humos instalado en el interior del conducto.

Su aplicación básica será como elemento compartimentador y de cierre de los conductos de climatización y ventilación.

Medios complementarios. Debido a la gran importancia que adquiere el comportamiento de diferentes elementos constructivos, materiales y equipos durante la manifestación de un fuego, a continuación se indican aquellos de características especiales, cuya adecuación mejorará los niveles de compartimentación del edificio.

En cuanto a *elementos constructivos*, cabe destacar:

- *Cámaras, conductos y espacios ocultos:* su paso a través de elementos compartimentadores ha de recibir un adecuado tratamiento constructivo.
- *Cajas verticales para instalaciones y servicios:* han de estar compartimentadas con un valor de resistencia al fuego de, al menos, el 50 por ciento del que ofrezcan los forjados que atraviesan; y el cerramiento y el acabado interior deben ser de materiales incombustibles.
- *Conductos de climatización o ventilación:* deberán disponer de compuertas cortafuego en todo punto de paso por un elemento compartimentador.
- *Pasos de tuberías, conductos y cables:* su paso a través de elementos compartimentadores debe realizarse mediante la menor perforación posible y

sellando la holgura existente mediante materiales o elementos estables e incombustibles.

- *Revestimientos de paramentos horizontales o verticales.*

En cuanto a *materiales y equipos* principalmente destacan:

- *Cables antifuego:* para protección de la instalación eléctrica que cumplan las características de no propagación de la llama, no propagación del incendio, reducida emisión de gases tóxicos, nula emisión de gases corrosivos, baja emisión de humos opacos y resistencia al fuego. Los cables, igualmente, pueden tratarse ignífugamente mediante recubrimientos ablativos.

- *Sellado de canalizaciones:* cualquier hueco que comunique dos áreas pertenecientes a sectores de incendios contiguos ha de ser sellado para retardar el paso del fuego y proporcionar la estanquidad de humos, gases, polvo, productos químicos, etc. Esto se realiza mediante materiales aislantes como lana de roca sostenida por una malla metálica, bolsas obturadoras, elementos cortafuegos modulares, masillas intumescentes, espuma de silicona, etc.

- *Motorización de compuertas y sistemas de mando y control:* la compuerta cortafuego actúa como una unidad compacta.

- *Conductos de ventilación resistentes al fuego:* mediante el revestimiento de los conductos de chapa metálica con placas incombustibles, libres de amianto, que pueden proporcionar una resistencia al fuego de hasta 4 horas.

• **Evacuación de humos**

La evacuación de humos se establece mediante *la adopción de medios y medidas de seguridad para conseguir que el humo producido por un incendio no invada toda la zona y provoque la asfixia de las personas que se encuentran en el interior del recinto.*

La evacuación de humos y calor de la zona en la que se produce un incendio, principalmente se puede realizar:

- *Estáticamente.* Mediante compuertas o lucernarios de cubierta que se abren automática o manualmente. Solución para aplicación en los edificios de una planta, patios y huecos de escaleras.
- *Dinámicamente.* Mediante sistemas de activación de aireación. Solución para aplicación en edificios de varias plantas.

Los principales *objetivos* a conseguir con la implantación de sistemas de evacuación de humos son:

- Proteger a las personas del humo.
- Evacuar el humo, calor y gases.
- Evitar la extensión lateral del incendio.
- Favorecer la actuación de los medios de extinción e intervención.



Los dispositivos, equipos y sistemas que conforman el subsistema de evacuación de humos, principalmente son:

- Barreras contra el humo.
- Exutorios.
- Ventiladores para los conductos.
- Campanas extractoras de humos.

Barreras contra el humo. En el caso de incendio en un edificio comercial de grandes dimensiones es vital conseguir que el humo no invada la totalidad del volumen, y que sea conducido al exterior por el camino más corto posible.

Las barreras contra el humo *según su tipo de instalación y función*, pueden ser:

- *Fijas:* compuestas por un perfil de sustentación y una fibra textil especial, impermeable al humo y resistente a altas temperaturas.
- *Automáticas enrollables:* pueden quedar ocultas en el falso techo del recinto comercial y caer controladamente en caso de incendio y activadas automáticamente por sistemas de detección de humos.
- *Creadoras de sectores de humo:* evitan que el humo se enfríe al alejarse del origen del incendio.
- *Canalizadoras:* reducen el frente de la columna de humo ascendente y evitan que las plantas superiores se llenen de humo.
- *Delimitadoras:* evitan que el humo ascienda por volúmenes de comunicación entre plantas e invada zonas no afectadas.

Exutorios. Son *dispositivos para la evacuación de humos y gases de forma natural que cumplen las funciones de aireación natural, ventilación, evacuación dominada de los humos y gases, e iluminación natural.*

Un exutorio de humos está constituida por una parte fija (unida solidariamente a la cubierta del edificio) y una parte que se abre (articulada sobre el elemento fijo).

El otro componente del exutorio es el sistema de mando a distancia para su apertura y/o cierre que puede ser activado por: sistema fusible al alcanzar una determinada temperatura, por sistema de detección de humos y por disparo manual.

Ventiladores para los conductos. Los ventiladores para los conductos de extracción y presurización de huecos de escalera son los *dispositivos de suministro de*

aire fresco y limpio, que insuflan la cantidad necesaria a fin de mantener el nivel de presión y/o la velocidad del aire requeridas.

Los ventiladores son los equipos básicos para el diseño de un sistema de presurización mediante el que se consiga controlar el movimiento del humo.

Campanas extractoras de humos. Son *equipos diseñados para la evacuación mecánica de humos y gases, instalados en las cubiertas de los edificios.* Generalmente se componen de base, caperuza construida con material tratado específicamente contra el fuego y motor ventilador.

3.1.6 EXTINCIÓN DE INCENDIOS

El sistema de extinción de incendios se define como el *conjunto de equipos o sistemas tendentes a ofrecer una instalación adecuada para la lucha contra el fuego.*

Dentro de los medios pasivos de extinción de incendios aplicables a los establecimientos comerciales, tenemos:

Agentes extintores.

Medios manuales de extinción.



- **Agentes extintores**

Agente extintor es el producto o compuesto que al ser proyectado sobre un fuego provoca la extinción del mismo.

Atendiendo a su estado físico los agentes extintores **se clasifican** en:

- Líquidos:

- Agua.

- Agua con aditivos.

- Espumas.

- Sólidos:

- Polvo químico seco BC.

- Polvo químico seco ABC.

- Gaseosos:

- Dióxido de carbono.

- Otros agentes extintores gaseosos.

Existe una *adecuación de los agentes extintores* a cada una de las clases de fuego.

- **Agentes extintores líquidos.** Se consideran agentes extintores líquidos los siguientes:

- *Agua.* Es el agente extintor más utilizado. Al alcanzar su punto de vaporización, el vapor producido desplaza el aire que rodea el fuego y, por tanto, el oxígeno

que actúa de combustible. Al ser más pesada que la mayoría de los combustibles líquidos, el agua no es efectiva en la extinción de fuegos de líquidos.

- *Agua con aditivos.* La mejora de la efectividad del agua como agente extintor se consigue añadiéndole aditivos específicos:

Humectantes. Facilitan la penetración del agua.

Espesantes. Extinción más efectiva del fuego por sofocación.

Anticongelantes. Reducen el punto de congelación del agua.

- *Espumas.* Genéricamente *la espuma es una masa de burbujas obtenida al introducir aire en una solución espumante, que aplicada sobre la superficie del combustible incendiado, forma una capa que lo aísla del comburente, extinguiendo el fuego por sofocación.*

En función de su coeficiente de expansión (relación entre el volumen de espuma producida y el volumen de espumante necesario para producirla) se clasifican en:

De baja expansión. Muy sólidas y resistentes, con ellas se consiguen grandes distancias de lanzamiento (próximas a las del agua).

De media expansión. Más ligeras, alcances menores (5 o 6 metros).

De alta expansión. Muy ligeras, su alcance es mínimo.

El empleo fundamental de las espumas es contra fuegos de líquidos inflamables, pudiéndose utilizar también en fuegos de combustibles sólidos. No son eficaces en fuegos de gases ni fugas de líquidos a presión.

- **Agentes extintores sólidos.** Se consideran agentes extintores sólidos los siguientes:

- *Polvo químico seco.* El polvo químico seco está formado por partículas finas (polvo) de sustancias inorgánicas (químico) sin humedad, que puedan producir grumos (seco) para que tenga fluidez en su proyección al fuego.

Los tipos de polvo químico seco son:

Polvo químico seco BC. Compuesto fundamentalmente por bicarbonato sódico y tetraborato sódico, apropiado para la extinción de fuegos de las clases B y C.

Polvo químico seco polivalente. Compuesto fundamentalmente por fosfato monoamónico, apropiado para la extinción de fuegos de las clases A, B y C.

El polvo químico seco no es buen conductor de la electricidad, no siendo recomendable la utilización de BC para tensiones superiores a 5.000 voltios y el ABC para tensiones superiores a 1.000 voltios.

El empleo del polvo químico seco no es compatible con la utilización de espumas.

- **Agentes extintores gaseosos.** Se consideran agentes extintores gaseosos los siguientes:

- *Dióxido de carbono.* Aprovecha la propia presión de almacenamiento para su impulsión al fuego. Al ser un gas tiene mayor capacidad de penetración. No es buen conductor de la electricidad, por lo que se convierte en el agente extintor ideal para fuegos en presencia de tensión eléctrica. Para fuegos clase A y B se aplica en sistemas fijos por inundación total o aplicación local.

En las mismas condiciones que el aire, tiene una densidad del 50 por ciento superior, por lo que al desplazar el aire y, por tanto, el oxígeno se convierte en un producto asfixiante (en concentraciones superiores al 9 por ciento). Es necesario tomar las debidas precauciones cuando se utiliza en recintos cerrados con presencia de personas.

- *Otros agentes extintores gaseosos.* Como consecuencia de la prohibición de fabricar gases halones, debido al Protocolo de Montreal y su posterior ampliación en Copenhague, los fabricantes de agentes sustitutivos se centran en encontrar una alternativa que cumpla los siguientes requisitos: no estar afectados por el Protocolo de Montreal, bajo impacto ambiental, eficacia de extinción similar al

halón, toxicidad baja para el hombre, exigencias indicadas por la EPA, ser económicos y poder sustituir al halón en las instalaciones existentes, con ninguna o pocas modificaciones.

• Medios manuales de extinción

Extintores móviles. Los extintores son aparatos que contienen un agente extintor que puede ser proyectado y dirigido sobre un fuego por la acción de una presión interna.

Un extintor portátil es un extintor concebido para ser llevado y utilizado a mano y que, en condiciones de funcionamiento, tiene una masa inferior o igual a 20 kg.

La carga de un extintor es la masa o el volumen del agente extintor contenido en su interior. Desde el punto de vista cuantitativo, la carga de los aparatos a base de agua se

expresa en volumen (litros) y la de los restantes aparatos en masa (kilogramos).



Según la carga los extintores se clasifican en:

- *Extintores portátiles manuales.* La masa total transportable es igual o inferior a 20 kg y *extintores portátiles dorsales*, cuya masa total transportable es igual o inferior a 30 kg. Están equipados con un sistema de sujeción que permite su transporte a la espalda de una persona.

- *Extintores sobre ruedas.* Son aquéllos que están dotados de ruedas para su desplazamiento.

En las normas tecnológicas se establecen las características que deben cumplir los extintores portátiles.

Elección del agente extintor. El agente extintor debe ser apropiado a la clase de fuego que vaya a combatir, es decir, a los combustibles existentes y las operaciones industriales que existan en el riesgo, con el fin de que su acción se manifieste como más eficaz.

Además, en el momento de la elección del agente extintor, hay que tener en cuenta la posible toxicidad de los gases producidos en la descomposición por el calor de algunos agentes extintores cuando se emplean en locales pequeños o mal ventilados.

Debe considerarse también la posibilidad de dañar a equipos sensibles o delicados (aparatos de refrigeración, electrónicos, equipos mecánicos, ópticos de precisión, etc.).

Emplazamiento de los extintores. Los extintores manuales se deben colocar sobre soportes fijados a parámetros verticales o pilares, de forma que la parte superior del extintor no exceda de una altura de 1,70 m.

Su distribución en el riesgo a proteger será:

- En áreas con posibilidad de fuegos clase A, distancia máxima a recorrer un extintor, 25 m.
- En áreas con posibilidad de fuegos clase B, distancia máxima a recorrer un extintor, 15 m.
- Para protección de transformadores y disyuntores que contengan aceite combustible, así como de las calderas que tengan quemadores alimentados por electricidad, deberá existir, como mínimo, un extintor de polvo de 6 kg o 2 extintores de CO₂ de 5 kg cada uno, a más de 3 m y menos de 15 m de los riesgos citados.

Bocas de Incendio Equipadas (BIE). Es el conjunto de elementos necesarios para transportar y proyectar agua desde un punto fijo de una red de abastecimiento de agua hasta el lugar del fuego.

Las normas tecnológicas establecen las características que deben cumplir las instalaciones fijas de extinción de incendios. Sistemas equipados con mangueras. Bocas de incendio equipadas con mangueras semirrígidas y planas.

Abastecimiento de agua. El abastecimiento de agua para las instalaciones de BIE será, como mínimo, de tipo sencillo, con capacidad para alimentar a la instalación, al menos durante 60 minutos, en las condiciones de caudal y presión previstas para cada caso y riesgo.

Se podrá alimentar la instalación de BIE desde una red general de incendios común a otras instalaciones de protección, siempre que en el cálculo del abastecimiento se hayan tenido en cuenta los mínimos requeridos por cada una de las instalaciones que han de funcionar simultáneamente.

Emplazamiento y distribución. Las BIE deberán situarse en los paramentos o pilares de los locales, de forma que el centro de la misma quede a una altura inferior a 1,5 m con relación al suelo; y al menos una por planta, cerca de las puertas o salidas, aunque sin constituir obstáculo para la utilización de éstas.

En las BIE de 25 mm, la altura sobre el suelo podrá ser cualquiera, siempre que la boquilla y la válvula se encuentren a una altura máxima de 1,50 m con relación al suelo.

La determinación del número de BIE y su distribución se hará de tal modo que la totalidad de la superficie a proteger lo esté al menos por una BIE, considerando un alcance nominal de 6 y una separación máxima entre cada BIE y su inmediata más cercana de 50 m.

La distancia desde cualquier punto del local protegido hasta la BIE más próxima no deberá exceder de 25 m, procurando mantener alrededor de cada una amplias zonas libres de obstáculos que permitan el acceso y maniobra sin dificultad.

Hidrantes exteriores. Son aparatos hidráulicos, conectados a una red de abastecimiento de agua y destinados a suministrar agua en caso de incendio en todas las fases del mismo.

Clasificación en función de su *diseño y aplicación*:

- Hidrantes de columna (CHE):

De columna seca.

De columna húmeda.

(la diferencia estriba por el hecho de que el cuerpo de la columna se encuentre ocupado, o no, por agua cuando el hidrante no está siendo utilizado).

- Hidrantes bajo nivel de tierra:

Húmedo.

Seco.

Clasificación en cuanto a sus *dimensiones*:

- Hidrantes de columna:

Hidrantes de 80 mm provistos de 2 bocas de 45 mm y una boca de 70 mm de diámetro nominal.

Hidrantes de 100 mm y 150 mm provistos, al menos, de 2 bocas de 70 mm y una boca de 100 mm de diámetro nominal.

- Hidrantes bajo nivel de tierra:

Boca de 45 mm.

Boca de 70 mm.

Boca de 100 mm.

Boca de 150 mm.

Las normas tecnológicas establecen las características que deben cumplir los hidrantes de columna seca, hidrantes de columna húmeda e hidrantes bajo nivel de tierra, respectivamente.

Abastecimiento de agua. Un sistema de abastecimiento de agua es el formado por los siguientes componentes: una o varias fuentes de alimentación de agua, uno o varios sistemas de impulsión y una red general de distribución a las distintas instalaciones que alimente. Además, debe asegurar, para uno o varios sistemas específicos de extinción de incendios, el caudal y presión de agua necesarios durante el tiempo de autonomía requerido.

Un sistema de abastecimiento de agua puede no necesitar mantener las condiciones de caudal y presión requeridas si la fuente de alimentación de agua de por sí las reúne.

Sistema de impulsión. Corresponde al conjunto de medios o circunstancias naturales que permite mantener las condiciones de presión y caudal requeridas.

Red general de distribución. Se refiere al conjunto de tuberías, válvulas y accesorios que permite la conducción del agua desde la salida del sistema de impulsión hasta los puntos de alimentación de cada sistema específico de extinción de incendios.

Puede no existir en los casos en que sólo se alimente un sistema específico de extinción.

Tipos de fuentes de alimentación

- Red de uso público.
- Inagotables: naturales (río, lago, mar, etc.) y artificiales (canal, embalse, pozo, etc.).
- Depósitos: bajo superficie, de superficie, elevados y de presión.



3.1.7 EMERGENCIA Y EVACUACIÓN

La protección y evacuación de emergencia la constituye el *conjunto de medios y dispositivos destinados a facilitar la evacuación de las personas, además de lograr la eliminación de trabas arquitectónicas de los propios edificios.*

Entre los principales dispositivos y materiales que conforman el subsistema de evacuación de aplicación en los establecimientos comerciales cabe destacar:

Las cerraduras y dispositivos antipánico, a instalar en huecos de paso.

La iluminación y señalización de emergencia, para las vías de evacuación.

Los equipos de protección personal contra el fuego.

Las mantas ignífugas.

• Cerraduras y dispositivos antipánico

Cerraduras. Estos dispositivos se instalarán fundamentalmente en los huecos de paso de elementos compartimentadores y a lo largo de las vías de evacuación. Según exigencias, dispondrán de la correspondiente homologación en cuanto a su grado de resistencia al fuego, de modo que quede garantizada la apertura y sea imposible su bloqueo ante su exposición al fuego.

Dispositivos antipánico. Consisten en dispositivos colocados en las puertas que permiten, mediante presión, la apertura de la puerta hacia el exterior, proporcionando una evacuación segura, rápida e impidiendo las aglomeraciones peligrosas que se pueden producir en los puntos de evacuación.

Las *funciones básicas* que deben satisfacer los sistemas antipánico, son:

- La puerta debe abrirse hacia el exterior.
- El sistema debe liberarse con una suave presión (como la que pueda ejercer un niño).
- La presión liberadora debe ser efectiva sobre cualquier punto de la barra antipánico ya sea ejercida de frente o de arriba hacia abajo.
- Posibilidad de condenar con total garantía el sistema de cierre por la parte exterior.

• Iluminación y señalización de emergencia

La iluminación de emergencia es aquella que permite guiarse fácilmente por un establecimiento en ausencia de la iluminación normal, de la que es totalmente independiente.

La señalización, por el contrario, es el conjunto de estímulos que informan a un individuo acerca de la mejor conducta a seguir ante una determinada circunstancia. En el caso de la señalización de seguridad, nos aportará la información general sobre los medios de alarma, las rutas de evacuación, la situación de los equipos contra incendios

y las zonas con riesgos especiales. No elimina el peligro en sí, pero aporta información sobre los procedimientos y normas a seguir en caso de emergencia.

En caso de producirse una emergencia, se deberá contar con una serie de dispositivos iluminadores y señalizadores que indiquen las rutas a seguir, tanto para personal conocedor de las instalaciones como para aquéllos que las visitan por primera vez.

Toda instalación comercial cuya ocupación pueda ser superior a 100 personas debe contar con iluminación de emergencia. Igualmente, debe instalar este tipo de iluminación en escaleras, pasillos protegidos, en todas las escaleras de incendios y en las rutas de evacuación.

En los aparcamientos de los grandes formatos comerciales se iluminarán los recorridos hasta el exterior o hasta las zonas generales del edificio.

Igualmente, los medios de protección contra incendios de utilización manual, que no sean fácilmente localizables, deben señalizarse de tal manera que sea visible desde cualquier punto de la zona protegida, para que pueda ser identificado de forma inmediata.

La iluminación de emergencia puede realizarse mediante equipos autónomos o mediante sistemas de alimentación ininterrumpida (S.A.I.) que aportan energía a las luminarias.

Otro tipo de iluminación de seguridad lo constituyen los equipos de balizamiento, que iluminan zócalos, escalones y huecos, lo que permite una evacuación segura.

Las señales fotoluminiscentes permiten señalar las vías de evacuación en caso de falta de suministro eléctrico, evitando las indecisiones e inseguridades que pueden generar retrasos e, incluso, pánico en caso de evacuación por emergencia.

- **Equipos de protección personal contra el fuego**

Equipo de protección personal es cualquier equipo destinado a ser llevado o sujetado por el trabajador para que le proteja de uno o varios riesgos que pueden amenazar su seguridad o su salud, así como cualquier complemento o accesorio destinado a tal fin.

La protección de las personas en presencia del fuego se puede conseguir mediante el uso de equipos de protección individual, especialmente indicados para las personas que han de intervenir activamente como componentes de los equipos definidos en el Plan de Emergencia del formato comercial (equipos de primera y segunda intervención).

Los equipos de protección personal contra el fuego básicamente pueden ser: cascos, pantallas faciales y gafas, para protección de la cabeza y la cara; guantes y botas, para protección de manos y pies; y trajes y equipos de respiración, para protección del cuerpo y las vías respiratorias.

Las *cualidades que han de valorarse* en los tejidos y en los equipos con ellos fabricados, para obtener una adecuada protección, son:



- *Características mecánicas:* resistencia al envejecimiento, resistencia al desgarrar, resistencia a la tracción, resistencia a la perforación, resistencia al impacto, flexibilidad y peso ligero.
- *Características térmicas:* resistencia a la llama, resistencia al calor radiante, aislamiento térmico, no desprendimiento de gases tóxicos por la acción del calor o llamas, fusibilidad.

Las *características generales* que deben cumplir las diferentes prendas o equipos de protección personal, en función de la parte del cuerpo a proteger, son:

- Protección de la cabeza y la cara.

Cascos: deberán ser resistentes a los impactos, al calor y al contacto con llamas y proporcionar un buen aislamiento térmico de la cabeza.

Pantallas faciales: no reducirán el campo visual, serán resistentes al choque térmico y proporcionarán un buen aislamiento frente a la radiación térmica.

- Protección de las manos.

Guantes: deberán proporcionar protección frente a la transmisión del calor por radiación, convección y conducción, y poseer buena resistencia mecánica y flexibilidad.

- Protección de los pies.

Botas: deberán ser resistentes a la inflamación o combustión por contacto con superficies u objetos calientes y proporcionar un buen aislamiento térmico y mecánico y serán resistentes al punzamiento o perforación.

- Protección del cuerpo.

El aislamiento térmico deberá estar reforzado en los puntos en contacto con el cuerpo; no deberá incrementar apreciablemente la producción de calor metabólico y deberá poseer un sistema rápido de apertura y cierre y no tener bolsillos exteriores.

- Protección de las vías respiratorias.

Deberán usarse exclusivamente *equipos de respiración autónomos de aire comprimido*.

- Protección integral.

Estos equipos se llevarán sobre la ropa de trabajo. Deberán poseer una buena resistencia mecánica y proporcionar un alto grado de protección frente a la radiación térmica y las llamas. Deberán ser impermeables.

- **Mantas ignífugas**

Las mantas ignífugas son elementos que permiten reaccionar con rapidez y eficacia ante situaciones de fuego, sofocando las llamas o evitando que prendan en personas u objetos.

De los diferentes tejidos y productos con que están fabricadas y tratadas las mantas ignífugas podemos destacar: de fibra de vidrio, de nomex, de lana y tratadas con gel para aliviar las heridas producidas por quemaduras.

3.2 SISTEMAS DE SEGURIDAD ACTIVA

Definimos genéricamente como sistema de seguridad activa a aquellos equipos y sistemas de seguridad de carácter electrónico que se pueden emplear, desde un punto de vista activo, para la prevención y la protección ante los riesgos y amenazas de los establecimientos comerciales. Entre los principales sistemas de seguridad activa se encuentran:

- **Control de accesos e identificación**
- **Protección contra hurto, robo y atraco**
- **Protección ante la agresión**
- **Protección de información y valores**
- **Protección contra incendios**
- **Extinción automática**
- **Control y emergencia**



3.2.1 CONTROL DE ACCESOS E IDENTIFICACIÓN

El control de accesos, en cuanto a los medios técnicos activos se refiere, es el conjunto de dispositivos a implantar para la comprobación, inspección, intervención o fiscalización del paso o circulación de personas, vehículos u objetos a una zona o recinto previamente definido como área de control o de seguridad para la prevención y protección ante riesgos que puedan afectar a personas, bienes y/o instalaciones.

Entre los principales equipos y sistemas de seguridad activa para el control de accesos de aplicación en áreas comerciales, se encuentran:

Los equipos de control e identificación de personas, para empleados, visitas y proveedores.

Los sistemas de tratamiento e identificación de matrículas.

• Equipos de control e identificación de personas

Es el conjunto de equipos o sistemas que de forma automática es capaz de: identificar a las personas que pretenden acceder a un recinto controlado, impedir el acceso a las personas no identificadas y autorizadas, jerarquizar los accesos a zonas determinadas, obtener información, y conocer instantáneamente los intentos no autorizados de acceso.

En función de su capacidad, complejidad y aplicación, el control de accesos puede ser: **autónomo**, que no tiene comunicación directa con un puesto de control, aunque puede disponer de canal de comunicaciones para volcar la información a una impresora o mando programador; y **centralizado**, que consiste en equipos distribuidos a lo largo del edificio o recinto y unidos entre sí, de forma que toda la información pasa por un puesto controlador y de supervisión de todo el edificio.

En los sistemas centralizados existen dos **filosofías de aplicación**:

1. Que el sistema precise confirmación para el acceso (interrogando a la base de datos del ordenador). Con esta exigencia, si la instalación cuenta con numerosos lectores y/o usuarios, el sistema puede ralentizarse mucho, incluso llegando a bloquearse en las horas punta, al tener que esperarse confirmación una vez presentada la tarjeta.

2. Que los equipos tengan su base de datos y las correspondientes parametrizaciones, lo que agiliza considerablemente el sistema en respuesta y efectividad, ya que el puesto de control puede dedicarse a otras actividades.

Un control de accesos de personas está formado por tres **elementos básicos**:

- *C.P.U. (Unidad Central de Procesos)*. Es la parte inteligente del sistema. En ella almacenan los datos los periféricos exteriores asociados al sistema (puertas, alarmas, barreras, torniquetes, etc.). Su ubicación será siempre dentro del recinto controlado para evitar su violación. Es importante que la *C.P.U.* sea independiente de la tecnología del lector y las tarjetas asociadas, basando su potencia en las posibilidades de control que posea.

- *Lector*. Es la parte encargada de descifrar la información contenida en la tarjeta o credencial y enviarla a la *C.P.U.* para su tratamiento. El lector y las tarjetas serán de la misma tecnología de fabricación.

Los requisitos más importantes que debe cumplir el lector para facilitar la labor del usuario son: robustez, señales acústicas y/u ópticas que indiquen el estado del sistema, *display* para información escrita, y versatilidad y facilidad de uso.

- *Credencial*. Con ella se identifica y diferencia a cada usuario dentro del sistema. Los diferentes tipos de credenciales a utilizar son:

Credencial material: tarjeta y/o emisor.

Credencial de conocimiento: teclado, cerradura y/o escritura.

Credencial personal: huella digital, geometría de la mano, voz, rasgos faciales y/o iris del ojo.

En función del nivel de seguridad deseado, se empleará un tipo de credencial o una combinación de varias.

Aplicación. El control de accesos de personas a áreas restringidas de los grandes formatos comerciales, en su más amplia concepción técnica, puede satisfacer las siguientes expectativas:

- Captación de imagen del rostro de la persona, para el diseño y fabricación, *in situ*, de credenciales en blanco y negro y color o como simple identificación a través de cámaras de CCTV.
- Controlar y gestionar adecuadamente un amplio número de credenciales, con la posibilidad de permitir o restringir el acceso a determinadas zonas del recinto.
- Posibilidad de ampliación de los equipos para dar respuesta a nuevas necesidades de implantación.
- *Software* único configurable, que permita la racionalización de medios técnicos y humanos, así como la gestión y control de accesos, presencia, visitas, horario, producción, rondas y alarmas.

- Posibilidad de integración con otros sistemas de seguridad y de gestión de la organización empresarial.

Parámetros de Selección. Dado que la implantación de un sistema de control de accesos puede ser complicada, es imprescindible un exhaustivo análisis de cada aplicación concreta, de acuerdo a los parámetros básicos siguientes:

- Definir los objetivos a alcanzar.
- Identificar las diferentes áreas de accesibilidad.
- Identificar los diferentes grupos humanos de accesibilidad.
- Definir el número y ubicación de los puntos de control de acuerdo a: elementos de identificación, elementos de control y necesidad de apoyo, o no, de otros medios (humanos, CCTV, etc.). Con el objetivo de conseguir: el menor número posible de puntos de control, la menor demora en el acceso, la mejor relación calidad/precio, y que interfiera lo menos posible en el funcionamiento normal del edificio o recinto en el que se implante.
- Definir las áreas de acceso: zonas de libre circulación y zonas restringidas.
- Definir los grupos humanos y horarios: en función de las misiones, responsabilidades, etc., de las personas (Director de Seguridad, personal de seguridad, de mantenimiento, directivos, empleados, visitantes, proveedores, etc.).
- Definir la tecnología de los equipos a implantar: en función del número de personas a controlar, picos máximos, nivel del riesgo, objetivos a alcanzar y aspectos estéticos y funcionales.
- Definir las medidas organizativas.

- **Sistemas de tratamiento e identificación de matrículas**

Es el conjunto de equipos o sistemas que de forma automática es capaz de identificar a los vehículos que pretenden acceder a un recinto controlado, obtener información y conocer instantáneamente los intentos no autorizados de acceso.

Aplicación. La adopción de estos sistemas permite incrementar el nivel de seguridad del recinto, gestionar de forma automática el reconocimiento de las matrículas, generando registros de información que contengan los datos de entradas, permanencias y salidas de los vehículos que acceden a la zona de muelles, almacenes generales y privados de un gran formato comercial.

Controles posibles

- Posibilidad de asociar a las matrículas de los vehículos la imagen del vehículo y la del conductor.
- Comparación del vehículo con la base de datos de autorizados con asignación de conductor.
- Contraste con un código (tarjeta magnética, de proximidad, etc.).
- Comprobación de fecha, día de la semana, horario en que el vehículo y conductor tienen permiso de acceso.

Operativa de control

Los datos que se pueden mostrar en el monitor a la llegada de un vehículo y conductor autorizados pueden ser los siguientes:

- Matrícula del vehículo.
- Marca, modelo y color del vehículo.
- Nombre, apellidos y D.N.I. del conductor asociado.
- Departamento de la empresa al que pertenece.
- Fotografía del conductor.

3.2.2 PROTECCIÓN CONTRA HURTO, ROBO Y ATRACO

La protección contra hurto, robo y atraco la conforman los *equipos y sistemas electrónicos capaces de alertar sobre situaciones delictivas*.

Entre los principales materiales y equipos de seguridad activa para protección contra el hurto, robo y atraco, de aplicación a los establecimientos comerciales, cabe destacar:

Los sistemas de detección, de especial protección contra la intrusión.

Las centrales de señalización y control, como elementos de control.

El centro de control, para centralización de los sistemas de seguridad.

La vigilancia por CCTV, para la captación y visionado de imágenes.

El etiquetaje y control antihurto, para protección de los artículos y mercancías en venta.

• Sistemas de detección

La detección es el conjunto de dispositivos que aseguran el conocimiento precoz de los hechos y alertan de situaciones irregulares, posibilitando una adecuada intervención para lograr frustrar la comisión de un delito.

La estructura básica de los equipos de detección, la componen tres bloques de



dispositivos conexcionados entre sí mediante elementos de comunicación. Estos tres bloques serían:

- Iniciadores
- Centrales
- Avisadores

El detector (iniciador) vigila una determinada área de cobertura y en caso de localizar una situación de alarma, transmite la correspondiente señal a la central. La central, en función de las señales recibidas de los detectores y de su propia programación, transmite las órdenes a los avisadores, para que éstos indiquen o retransmitan la situación de alarma.

Entre los principales equipos de detección, de aplicación en determinadas áreas de los establecimientos comerciales, cabe destacar:

- Detección interior.
- Detección exterior.

Detección interior. La detección interior la constituyen los *dispositivos de aplicación en áreas interiores*. En función de su zona de vigilancia, los detectores de interior se clasifican en:

- Puntuales.
- Lineales.
- Superficiales.
- Volumétricos.

Detectores puntuales. Para la aplicación en áreas comerciales, hemos de considerar los contactos magnéticos y los contactos mecánicos.

- *Contactos magnéticos.* Se fundamentan en que se detecta separación de dos piezas, imán y contactos, manteniendo el imán en cierta posición los contactos cuando está próximo a ellos.

De aplicación en la detección de apertura de puertas, ventanas, cajas, retirada de objetos, etc.

Presentan ventajas de sencillez de instalación, no precisan alimentación y presentan bajo índice de falsas alarmas y bajo coste.

Presentan inconvenientes de posibles sabotajes mediante imanes exteriores y posible intrusión por puerta o ventana sin abrirla.

- *Contactos mecánicos.* Se fundamentan en ser contactos eléctricos con reposición.

Su implantación es la misma que la indicada para los contactos magnéticos, fundamentalmente para instalar en espacios muy pequeños como en el interior de cerraduras.

Presentan ventajas como no precisar alimentación, bajo índice de falsas alarmas, difícil de ser detectado y bajo coste.

Presentan inconvenientes en cuanto al deterioro de los elementos mecánicos y posible intrusión por puerta o ventana sin abrirla.

Detectores lineales. Consideramos básicamente los rayos infrarrojos. Se fundamentan en el establecimiento de una línea imaginaria entre transmisor y receptor.

Su aplicación es para la detección de espacios largos y estrechos como pasillos, grandes escaparates, ventanales, etc. de los establecimientos comerciales.

Presentan ventajas de bajo índice de falsas alarmas y bajo coste.

Presentan inconvenientes de ser posible la intrusión sin detección, teniendo información exacta de su situación.

Detectores superficiales. Para la aplicación en áreas comerciales hemos de considerar las barreras de rayos infrarrojos, los detectores sísmicos, los detectores de rotura de vidrio.

- *Barreras de rayos infrarrojos.* Se fundamentan en la asociación de rayos infrarrojos situados paralelamente entre sí, de modo que la intervención de alguno de los haces genera la alarma.

Su aplicación es para la protección interior de amplios espacios superficiales, como las cubiertas de los edificios.

Presentan ventajas de bajo índice de falsas alarmas y las derivadas de su plano de cobertura.

Presentan inconvenientes en la dificultad de alimentación de los haces y coste elevado.

- *Detectores sísmicos.* La causa desencadenante para su activación es la



vibración. Son transductores que han tomado su nombre de las ondas sísmicas que se propagan a distintas velocidades y que se originan cuando se produce una perturbación en un sólido elástico.

La causa desencadenante es la vibración producida y propagada en el interior de masas (aceros, hormigones, etc.), cuando sufren ataque por elementos de percusión o térmicos. Convierte, mediante la utilización de micrófonos selectivos, vibraciones mecánicas en señales eléctricas.

Su aplicación es para la protección de muros de cámaras acorazadas, cajas fuertes y en general espacios de alto riesgo.

Presentan ventajas de gran sensibilidad, inmunidad ante vibraciones ambientales, bajo índice de falsas alarmas y posibilidad de comprobación de su estado desde la central.

- *Detectores de rotura de vidrio.* Son transductores activos preparados para recibir un estímulo de entrada –vibración, ruido, rotura, etc.– y proporcionar como respuesta una señal eléctrica de salida. Su elemento sensible, el sensor, normalmente es de tipo microfónico, piezocerámico o piezoeléctrico.

Su aplicación es para la protección de acristalamientos, detectando su rotura. En función del estímulo de entrada que detecten, según la tecnología de fabricación, se instalarán adosados al vidrio o a una determinada distancia del acristalamiento.

Detectores volumétricos. Para aplicación en áreas comerciales hemos de considerar los detectores de infrarrojos pasivos, de microondas, de ultrasonidos y detectores de tecnología dual.

- *Detectores de infrarrojos pasivos.* Se fundamentan en la detección de movimiento analizando las variaciones de la radiación infrarroja de los cuerpos en el ambiente.

Su aplicación es para la protección de un volumen interior.

La tecnología de fabricación, de algunas marcas, de este tipo de detectores ha minimizado los problemas iniciales de escasa sensibilidad, posibilidad de apantallamiento y posibilidad de falsas alarmas por presencia de pequeños animales.

- *Detectores de microondas*. Se fundamentan en la detección del movimiento de personas u objetos capaces de reflejar las señales, la emisión radioeléctrica emitida por el sensor en el espectro de las microondas (del orden de 10 Ghz).

Su aplicación es para la protección de un volumen interior.

Su empleo puede producir detecciones no deseadas por traspasar acristalamientos o paredes, por ello cobra especial importancia su ajuste en el momento de la instalación.

- *Detectores de ultrasonidos*. Se fundamentan en la detección del movimiento de personas u objetos capaces de reflejar las señales acústicas de alta frecuencia (ultrasonidos), emitidas por el sensor.

Su aplicación es para la protección de un volumen interior.

Es conveniente evitar su instalación en lugares donde existan o puedan producirse corrientes de aire.

- *Detectores de tecnología dual*. Los detectores volumétricos de tecnología dual están preparados para recibir dos estímulos de entrada y, por lo tanto, su activación se realiza por una causa desencadenante (movimiento) y dos principios operativos: 1. *Óptico y acústico* [infrarrojos pasivos + ultrasonidos (IR+US)]. 2. *Óptico y electromagnético* [infrarrojos pasivos + microondas (IR+MW)]. Se desarrollan en torno a dos filosofías completamente diferentes: los denominados de composición y los de correlación. En los de composición, la electrónica se caracteriza por la utilización, en el mismo detector, de dos sensores diferentes con distintos principios operativos: infrarrojos pasivos + microondas (IR+MW), o infrarrojos pasivos + ultrasonidos (IR+US), activándose la alarma del detector cuando uno de los sensores está en alarma (OR), o cuando los dos sensores, al mismo tiempo, sobrepasan unos umbrales

preestablecidos (AND). En los de correlación, el establecimiento de un *software* para el procesamiento de las señales permite discernir entre causas desencadenantes falsas y verdaderas, produciéndose una alarma cuando, al activarse uno de los sensores, pasa a situación de vigilancia y se concentra en lo que recibe a través de una especie de barrido. Si en esta situación comprueba con el otro sensor la perturbación real, se da la condición de alarma.

Por lo tanto, los detectores de tecnología dual son los volumétricos que mayores garantías ofrecen en la protección de volúmenes interiores, representando un mayor coste al incorporar dos sensores de diferentes tecnologías.

Detección exterior. La detección exterior la constituyen los *dispositivos de aplicación en áreas exteriores que delimitan una zona perimetral de protección*.

Los equipos más usuales para la detección exterior en áreas comerciales, son:

- Barreras de infrarrojos.
- Barreras de microondas.
- Sistemas para la protección de vallados.
- Sistemas enterrados.
- Videosensores.

Barrera de infrarrojos. Puede utilizarse para conformar un sistema de detección de intrusión, de emplazamiento exterior y zona de vigilancia de tipo lineal. La causa desencadenante para su activación es el movimiento del intruso y el principio operativo empleado es de tipo óptico. Podríamos definirla como una línea imaginaria no visible que une dos puntos –transmisor y receptor– y que, al ser interrumpida o atravesada, produce una señal de alarma en el extremo receptor.

Barrera de microondas. De emplazamiento exterior y zona de vigilancia tipo volumétrica, tiene como causa desencadenante la perturbación derivada del movimiento del intruso y su principio operativo es de tipo electromagnético.

De forma genérica, podemos decir que un oscilador en el transmisor genera una portadora de radiofrecuencia –RF en la banda X– que será modulada por una señal de audiofrecuencia. Una antena concentra la energía RF generada hacia el receptor. En éste se encuentra dispuesta una antena similar y, en el caso de que un intruso se introduzca en



el campo electromagnético existente entre el transmisor y el receptor, genera una modificación del campo que será evaluada por los circuitos electrónicos del receptor, activándose la alarma en caso de disminución de la intensidad de campo por debajo del valor umbral o sensibilidad preestablecida.

Sistemas para la protección de vallados. Están diseñados para su emplazamiento en exteriores y su zona de vigilancia es de tipo superficial. La causa desencadenante de su funcionamiento puede ser presión, rotura o vibración, y el principio operativo empleado es de tipo diferencial, óptico, eléctrico o electromecánico.

Los sistemas de detección por vibración en vallados con sensores aislados, detectan la vibración en los vallados por medio de detectores inerciales dispuestos sobre ellos y asociados en grupos de 100 a 200 metros cuyas señales se analizan conjuntamente. Su aplicación es sobre vallados metálicos de suficiente rigidez.

Los sistemas de detección por vibración en vallados con sensor (cable) continuo detectan las vibraciones por efecto piezoeléctrico, triboeléctrico capacitivo. Su aplicación es sobre vallados metálicos de suficiente rigidez.

En los sistemas de detección por cables de tensión, el sensor en sí mismo es un vallado, está formado por cables horizontales tensados, que terminan en sensores que detectan la variación de tensión mecánica. Su aplicación es como vallado metálico ante el corte, separación y escalada.

Sistemas enterrados. De aplicación para la protección del perímetro a través del suelo y de emplazamiento en exteriores, presentan una zona de vigilancia del tipo superficial. La causa desencadenante de su funcionamiento puede ser presión, rotura, vibración o movimiento, y el principio operativo empleado es de tipo diferencial, óptico, eléctrico o electromagnético.

Los sistemas de detección por presión en el suelo (hidráulicos), detectan la presión generada en el suelo por el paso de una persona, analizando la diferencia de presión generada en dos tubos que discurren bajo el suelo y paralelos entre sí. Su aplicación es en todo tipo de terrenos excepto los rocosos y arbolados.

Los sistemas de detección por sensores aislados, detectan la presión generada en el suelo mediante sensores sísmicos analógicos, tratando conjuntamente sus señales. Su aplicación es en todo tipo de terrenos excepto los rocosos y arbolados.

Videosensores. Son dispositivos detectores de movimiento que utilizan la variación de luz de una escena observada para activar una alarma de forma automática. La causa desencadenante para su activación es el movimiento del intruso y el principio operativo es de tipo óptico.

• Centrales de señalización y control

Se entiende por central de señalización y control *todo equipo autoprotegido, que integrado en un sistema electrónico de seguridad es capaz de recibir y controlar información y generar señales de comunicación con otros dispositivos.*

Los grandes **bloques funcionales** que conforman la centralización de alarmas en una instalación, son:

Alimentación. Este bloque conectado a la red eléctrica local o al suministro eléctrico primario, transforma y/o rectifica la corriente adaptándola a las necesidades del sistema de seguridad. Incluye las baterías para acumular energía de emergencia de capacidad adecuada al sistema controlado.

Este bloque o fuente de alimentación proporciona corriente eléctrica a los circuitos de la central, a las líneas de detectores y a los dispositivos de alarma.

Entradas. Está constituido por elementos o circuitos que permiten la entrada hacia el bloque de “Análisis y tratamiento de la señal” de las señales e informaciones procedentes de las líneas o bucles, a los que están conectados los diversos elementos de señalización de la información procesada o previamente programada.

Análisis y tratamiento de las señales. Evalúa la naturaleza de las señales recibidas, procedentes del bloque de “Entradas”, en función de los parámetros previamente establecidos, activando la alarma en caso de confirmarse las condiciones programadas.

Elementos de mando y control. Posibilitan el gobierno del sistema de seguridad y controlan su funcionamiento, respuestas, etc. Pueden ser locales (en el propio equipo) o remotos.

Contenedor. Es la caja, armario, *rack*, pupitre, etc., que encierra la circuitería de los distintos bloques anteriormente mencionados y a la vez sirve de soporte a los órganos de mando y control.

Comunicaciones. La comunicación entre los diferentes equipos (bloques) será vía radio (en el caso de los sistemas inalámbricos) o vía cable (en el caso de los alámbricos).

Salidas. Este bloque es el que permite la transmisión de señales a los avisadores o periféricos de recepción y gestión de alarmas.

Según su aplicación, las centrales pueden ser contra:

- Intrusión o robo.

- Atraco.
- Combinadas (intrusión, robo, atraco).
- Mixtas: siendo combinadas admiten detectores de otras funciones, tales como detección de fuego u otros.

Según su tecnología, las centrales pueden ser:

- Locales.
- Microprocesadas.
- De comunicación bidireccional.



• Centro de Control

El Centro de Control es *donde se conectan y gestionan los aparatos, dispositivos o sistemas de seguridad.*

Un Centro de Control ha de cumplir, al menos, **cuatro conceptos básicos** con garantía y eficacia; éstos son:

- Control permanente
- Verificación efectiva
- Capacidad de respuesta
- Seguridad requerida

El **control permanente** de las instalaciones remotas es uno de los principios básicos que debe cubrir un centro de control, así como el diálogo (recepción y transmisión) con los equipos de detección, telecontrol, telemando, etc.

Igualmente, ha de ofrecer con suficiente garantía la **verificación efectiva** de las incidencias acaecidas, tanto en forma como en tiempo real, gestionando con diligencia el resto del proceso operativo que se ha de realizar.

Dispondrá necesariamente de una adecuada **capacidad de respuesta** para posibilitar una inmediata reacción, gestión y resolución –según los servicios y niveles de seguridad– ante las incidencias o alarmas producidas. La atención simultánea de múltiples incidencias será uno de los factores determinantes de su capacidad de respuesta.

Ha de ofrecer con garantía la **seguridad requerida**, la exigida y la esperada para cada uno de los servicios ofrecidos y planeados. El cumplimiento satisfactorio de los conceptos de control permanente de las instalaciones remotas, de verificación efectiva de las incidencias o alarmas, y de capacidad de respuesta para su reacción o resolución, serán los principales factores de calidad y seguridad del Centro de Control.

El Centro de Control que se plantea para este tipo de instalaciones es propio de cada gran establecimiento comercial. Igualmente, un centro comercial poseerá uno propio (normalmente denominado Puesto Permanente de Seguridad) en donde se centralicen y gestionen todas las señales que provienen de los dispositivos de seguridad y protección instalados en todo el recinto.

El planteamiento de la seguridad en los grandes formatos comerciales pasa por la gestión general de todos los aspectos que conciernen a la misma, y por tanto, uno de los puntos básicos para el Director de Seguridad es la información.

Como ejemplo, si se considera una gran superficie que se encuentra en un centro comercial, se propone una estrecha colaboración entre los Directores de Seguridad respectivos, ya que, algunos de los riesgos relacionados en el catálogo de riesgos de ambos establecimientos, son los mismos en ambos casos. En muchos aspectos se enfrentan a la misma problemática y, por tanto, pueden realizar un frente de ataque común. Así, para la gran superficie se puede establecer que una serie de

señales de algunos dispositivos de seguridad tengan su correspondiente aviso en el Centro de Control del centro comercial y viceversa. Este es el caso de las señales de incendio, cuyo origen puede estar en un establecimiento pero su desarrollo afecta, o puede afectar, a la totalidad de la superficie.

• Vigilancia por circuito cerrado de televisión (CCTV)

Un sistema de CCTV consiste en la visualización remota de lugares vigilados. Está compuesto por un número limitado de pantallas y cámaras de televisión, en el cual la señal se distribuye mediante una red cerrada de interconexiones y que permiten captar y enviar imágenes desde un lugar a otro.

Son muchos y muy variados los equipos que pueden conformar el subsistema de vigilancia por CCTV. A continuación se definen brevemente, los de aplicación a establecimientos comerciales:

- Elementos de captación de imagen:

Cámaras de vídeo.

Ópticas.

- Elementos de control y comunicación:

Equipos de control.

Equipos de conmutación.

Elementos de comunicación.

- Elementos de alarma:

Videosensores.

- Elementos de visualización de imágenes:



Monitores de vídeo.

Equipos auxiliares de monitorización.

- Elementos de registro de imágenes:

Magnetoscopios.

Videoimpresoras.

Sistemas de almacenamiento digital de imágenes.

- Videograbación/transmisión digital de imágenes.

Cámaras de vídeo. La cámara es el elemento de partida de cualquier CCTV. Es el aparato electrónico encargado de convertir los cambios de luz y color de la escena enfocada en impulsos eléctricos que puedan ser transmitidos a distancia y que sirven para reconstruir una imagen en el lugar de control.

Ópticas. Elemento imprescindible en la captación de imágenes. Son las encargadas de la elección del campo visual que la cámara verá. El tipo de óptica se elegirá en función de diferentes variables: distancia focal, iluminación, etc.

Equipos de control. Son los que proporcionan diferentes posibilidades a los elementos de captación de imágenes: posicionadores, horizontales y/o verticales, interruptores de iluminación, controles de zoom, controles de iris, interruptores de cámara.

Equipos de conmutación. Son los que transforman las entradas de vídeo: amplificadores, distribuidores, conmutadores

manuales, secuenciadores, divisores de cuadrante, matrices de conmutación.

Elementos de comunicación. Son los que transportan la señal de vídeo a los equipos de visualización y al resto de elementos auxiliares: cable coaxial, cable de pares + ecualizador, enlace de microondas, láser, infrarrojos y fibra óptica.

Videosensores. Equipo de detección de movimiento basado en el análisis de los cambios de contraste de una escena filmada por una cámara cuando algún elemento de la imagen se desplaza por su campo de visión.

Monitores de vídeo. Constituyen el elemento de visualización de la imagen observada.

Equipos auxiliares de monitorización. Son los elementos auxiliares que intervienen en la visualización de imágenes: generadores de fecha y hora, eclipsador, micrófonos de audio, multiplexores.

La función principal de estos equipos es descargar al operador del centro de control de la tarea de observar continuamente las pantallas de los monitores que reflejan una escena fija.

Magnetoscopios. Son los equipos que permiten grabar, almacenar y reproducir las imágenes obtenidas del CCTV, mediante cinta magnética.

Videoimpresoras. Son los equipos que permiten imprimir fotogramas a partir de cinta magnética.

Sistemas de almacenamiento digital de imágenes. Archivan las imágenes en forma digital.

Videograbación/transmisión digital de imágenes. Mediante estos sistemas se puede controlar remotamente las diferentes instalaciones del establecimiento comercial desde un Centro de Telegestión Multimedia, Centro de Control Remoto o Central Receptora de Alarmas.

Los elementos del sistema de control instalados en cada punto a vigilar gestionarán, con la máxima fiabilidad, diversos tipos de señales, tanto propias de subsistemas de seguridad como de instalaciones técnicas, registrando toda esta información automáticamente y de forma periódica y transmitiendo cuando el usuario del sistema lo requiera o automáticamente cuando se produzca una alarma.

Igualmente, un sistema de control centralizado constituye un auténtico registro y almacenamiento de datos, incluyendo todas las operaciones y acciones, las

incidencias e imágenes que pueden facilitar la identificación de personas y la reproducción de situaciones críticas.

Prestaciones mínimas del subsistema de CCTV. La instalación de un sistema de vigilancia por CCTV en un centro comercial deberá responder a una serie de cuestiones básicas que permitirá conseguir el propósito deseado buscando el equilibrio entre coste y eficacia. El mejor diseño no requiere únicamente una selección individual de equipos de elevada calidad sino la uniformidad y/o equilibrio entre todos sus elementos.

• **Etiquetaje y control antihurto**

El etiquetaje y control antihurto lo componen aquellos dispositivos adosados a los productos a la venta que evitan el intento de sustracción de los mismos.

Aplicación. Los principales sistemas antihurto son de aplicación para establecimientos comerciales, distribución y almacenaje. Se aplican a productos en exposición y venta, de especial valor o facilidad de hurto.

Podemos destacar:

- Los etiquetajes mediante códigos de lectura.
- Los etiquetajes mediante sistemas por radiofrecuencia, electromagnéticos o magnéticos.
- Los detectores antihurto.
- Los sistemas de plaqueta o pinza antihurto por radiofrecuencia.

El sistema antihurto está compuesto por etiquetas, equipos de detección (antenas) y desactivadores o desacopladores de etiquetas.

El funcionamiento consiste en que las etiquetas colocadas en los artículos a proteger emiten una señal que activa el equipo detector. Cuando un producto

protegido con la etiqueta se aproxima al detector, éste produce una señal de alarma, indicando al vendedor que retire la etiqueta del artículo, si es que éste se ha vendido, o informando sobre la intención delictiva.

El control antihurto de aplicación en los establecimientos comerciales utiliza dispositivos de protección que se basan en tres tecnologías diferentes: el acustomagnetismo, el electromagnetismo y la radiofrecuencia.

Etiquetas con tecnología acustomagnética (AM). La etiqueta contiene unas hojas metálicas que vibran en presencia de un campo oscilante, produciendo un sonido único. Esto posibilita ampliar el paso de las antenas por encima de los dos metros y ausencia de falsas alarmas, ya que la señal es única. Esta tecnología permite activación y desactivación.

Para desactivar la etiqueta se desmagnetiza una de las dos hojas metálicas de manera que cambia el sonido. Las etiquetas son voluminosas para que pueda darse la vibración.

Etiquetas con tecnología electromagnética (EM). El electromagnetismo aprovecha la actuación de unas finas líneas u hojas metálicas que quedan expuestas a un campo magnético oscilante. La etiqueta genera un conjunto de armónicos cuando alcanza su estado de saturación que es específico para la etiqueta. Esta tecnología permite la activación y desactivación.

Para desactivar el dispositivo se debe magnetizar una capa magnética dura de manera que se modifique el leve comportamiento magnético.

Etiquetas con tecnología por radiofrecuencia (RF). La tecnología de radiofrecuencia consiste en una espiral y una cavidad que forman un resonador. La etiqueta, convenientemente sintonizada, vibra suavemente y el consumo de energía activa la alarma.

Para desactivar la etiqueta debe destruirse el circuito de forma que no sea posible ninguna vibración posterior.

Etiquetado en origen. En el mercado existen proveedores de etiquetas (adhesivas o rígidas) con circuitos de radiofrecuencia que permiten la reimpresión y contienen la

información de identificación del producto. Por un lado, permite conocer los datos del fabricante (si se ha incluido la etiqueta en el punto de fabricación), los datos de manipulación y distribución del producto, control de los stocks, precio, promociones, fecha de venta, inicio de la garantía, etc. Por otro, en caso de robo, cuál ha sido la historia de este producto desaparecido.

Este tipo de etiquetaje permite, además, evitar la venta de productos robados y contribuye a la mejora de la productividad, ya que no hay que destinar a personal interno a la colocación de las etiquetas, porque toda la información se encuentra en el circuito. Pueden quedar ocultos.

Esta protección en origen es una de las piezas clave para la prevención de la pérdida desconocida, pues abre la posibilidad de reducir costes a medida que se generalice el procedimiento, lo que en un futuro permitirá proteger mercancías de bajo valor.

3.2.3 PROTECCIÓN ANTE LA AGRESIÓN

La protección activa ante la agresión se define como la instalación de dispositivos eléctricos o electrónicos cuyo objetivo es evitar o minimizar las consecuencias de las agresiones a personas y/o bienes.

Entre los principales equipos y sistemas de seguridad, cabe destacar:



Los sistemas de pulsación de emergencia o antiatraco.

Los equipos de inspección y detección de armas, explosivos y metales.

- **Pulsadores de emergencia o antiatraco**

Los pulsadores antiatraco son dispositivos discretos situados en lugares ocultos a la vista de los posibles atracadores, que emiten una señal no sonora al centro de control de seguridad avisando de la comisión de este delito.

Estos dispositivos pueden ser de accionamiento manual (pulsador) o mediante presión del pie (pedal). También existen en el mercado otros tipos manuales de accionamiento mediante un punzón o bolígrafo que son apropiados para posibilitar el aviso de atraco en ciertos lugares (aseos, etc.). Se instalan normalmente en la pared ya que su aspecto es similar a un mecanismo eléctrico normal.

Igualmente existen dispositivos sensibles a la presión, como pueden ser alfombras camufladas para detectar intentos de intrusión y/o atraco.

La pinza para billetes, de montaje en el interior de cajas registradoras o cajones, avisa cuando se pretenden extraer los billetes de la caja sin haber desactivado el mecanismo.

- **Equipos de inspección y detección de armas, explosivos y metales**

Los equipos de inspección y detección de armas, explosivos y metales son aquellos que permiten detectar y/o identificar el material u objeto cuyo acceso se desea controlar o no permitir.

Aplicación. Los equipos de inspección para detección de armas, explosivos y metales son de aplicación en establecimientos comerciales en caso de aparición de una amenaza de riesgo o agresión confirmado.

En función del tipo de objeto a controlar y del equipo controlador utilizado, se puede establecer una clasificación y una correspondencia.

Detección de explosivos. La decisión de implantar equipos detectores o inspectores de explosivos es complicada y estará en función de variables como el precio, la conveniencia de implantar determinados métodos en el establecimiento

comercial, la tecnología, la diversidad de compuestos explosivos, la variedad en la presentación de los artefactos y, básicamente, en el análisis de los riesgos efectuado.

Detección de armas. El equipo se fundamenta en un generador/receptor de campo magnético que detecta variaciones en la recepción, debido a la presencia de objetos metálicos, conductores, en su proximidad.

En función de su **aplicación**, estos equipos pueden ser:

- Portátiles. Detección de armas u objetos metálicos en personas o en el interior de paquetes.
- Por paso. Arco para la detección de armas u objetos metálicos en personas.

El parámetro básico que se ha de tener en cuenta en el momento de seleccionar un detector de metales será el factor discriminación, característica que depende de otros factores: uniformidad del campo magnético de prospección, tipo de análisis de los metales de interés e inmunidad a las interferencias externas.

Equipos de inspección por rayos X. Estos equipos se fundamentan en la obtención de imágenes interiores de cuerpos opacos por proyección de rayos X emitidos a su través.

Son de aplicación a la inspección de paquetes para la búsqueda de armas, artefactos explosivos u otros materiales u objetos.

3.2.4 PROTECCIÓN DE INFORMACIÓN Y VALORES

La protección activa de información y valores consiste en *la implantación de sistemas de tratamiento del efectivo generado en los establecimientos comerciales.*

Entre los principales equipos y sistemas para la protección de información y valores cabe destacar:

Las instalaciones de transporte neumático, para envío de efectivo.

Los sistemas de detección de dinero falso, para su instalación en áreas de cajas y salas de conteo.

Los equipos de retardo y bloqueo.

• **Transporte neumático**

El transporte neumático consiste en un sistema de tuberías por las que se desplaza el efectivo o documentos de forma que no permite la interrupción de su recorrido hasta su destino.

Aplicación. Para la protección del efectivo que se maneja en los establecimientos comerciales se utilizan instalaciones de transporte neumático que permiten automatizar y agilizar los trámites y desplazamientos del efectivo, y suponen un ahorro en tiempo y en personal.

Básicamente estas instalaciones se componen de un soporte contenedor (cartucho transportador) que es impulsado a gran velocidad por medio de aire por el interior de un tubo de PVC rígido, estabilizado y calibrado, como sistema de tuberías y un motor impulsor.

Aplicado a los establecimientos comerciales, el transporte neumático permite el envío de documentaciones o recaudaciones parciales desde las cajas de atención al público hasta la caja central, sala de conteo, caja fuerte o cámara acorazada.

Este sistema supone un desplazamiento físico seguro y rápido y evita errores humanos al ser de acceso directo.

Para determinar la idoneidad de una instalación de este tipo han de establecerse una serie de cuestiones básicas:

- Determinación de pesos máximos a soportar por el cartucho transportador (dinero metálico o papel moneda).
- Determinar los flujos unidireccionales o bidireccionales.
- Determinar el trazado de la instalación: interior o exterior.

- Determinar estaciones y frecuencia de envíos.
- Determinar calibres, recorridos, longitudes máximas y direccionamientos.
- Determinar el esquema básico de la instalación: todos con todos o todos con punto central.

• **Detección de dinero falso**

La detección de dinero falso consiste en comprobar, mediante diferentes dispositivos de tipo luz ultravioleta, que el efectivo recogido en las operaciones comerciales es auténtico.

Aplicación. Los equipos detectores de dinero falso son de aplicación en los establecimientos comerciales en todos los puntos de admisión de dinero.

Los billetes españoles cuentan con ciertas medidas de seguridad que hacen difícil su falsificación. La primera consiste en el soporte: el papel, que está elaborado en la Fábrica Nacional de Moneda y Timbre de Burgos y utiliza como materia prima la fibra de algodón. Su utilización está motivada por su alta resistencia y su capacidad para incorporar en su estructura ciertos elementos de seguridad como son:

- La marca de agua.
- El hilo de seguridad.
- Las fibrillas luminiscentes.
- El papel.
- El motivo coincidente.
- La leyenda microimpresa.
- La estampación calcográfica.



La marca de agua. Consiste en un dibujo formado por diferentes grosores del papel durante el proceso de elaboración. Se ve fácilmente al observar el papel al trasluz.

Hilo de seguridad. Se trata de una tira de material sintético especial de color verde embebida en la masa del papel durante el proceso de fabricación que cruza el billete en sentido transversal. Puede ser apreciado porque presenta un ligero relieve.

Fibras luminiscentes. Son fibras de material sintético que están incorporadas a la masa del papel a simple vista no se perciben, pero sí cuando son expuestas a luz ultravioleta. Su distribución es aleatoria e irregular a lo largo del papel.

Papel exento de blanqueante óptico. Al carecer de blanqueante óptico el papel de un billete no modifica su tono si se le expone a luz ultravioleta, esto permite que las fibrillas luminiscentes destaquen sobre el fondo del papel.

Motivo coincidente. Es el único motivo que es igual en el anverso y reverso del billete y coincide en el mismo punto en ambas caras. Se aprecia observando el billete al trasluz.

Leyenda microimpresa. En el borde de los fondos estampados de ambas caras figura una leyenda muy pequeña, "Banco de España", que se puede leer con la ayuda de una lupa.

Estampación calcográfica. Consiste en una estampación en relieve que se aprecia al pasar la yema del dedo o la uña por cualquier motivo.

En los centros de manipulación de efectivo existen diferentes máquinas de conteo que pueden determinar la autenticidad de las monedas (por diferencias de peso, normalmente) o de los billetes (por exposición a luz ultravioleta). En las líneas de caja o en los puntos de admisión de dinero se debe disponer de lámparas de luz ultravioleta por su comodidad y rapidez en la identificación.

- **Equipos de retardo y bloqueo**

Los equipos de retardo y bloqueo son básicamente relojes que temporizan la apertura de los dispositivos a los que van adosados.

Aplicación. Se utilizan en cajas fuertes, cajeros automáticos, cámaras acorazadas, etc.

Su mecanismo básico consiste en un reloj que dispone de un teclado (con o sin display) mediante el que se introduce la programación de la apertura, así como otras funciones adicionales: bloqueo por coacción, tiempos de apertura, memoria de eventos, conexión para la gestión desde equipos informáticos, etc.

Estos dispositivos cuentan con baterías internas que los convierten en equipos autónomos independientes de la corriente eléctrica. Igualmente tienen posibilidad de conexión al sistema de alarma.

3.2.5 PROTECCIÓN ACTIVA CONTRA INCENDIOS

La protección activa contra incendios es el conjunto de medios, equipos y sistemas instalados para alertar sobre un incendio e impedir que éste se propague evitando las pérdidas y daños producidos por el fuego.

Entre los principales equipos, sistemas e instalaciones de aplicación a este tipo de actividad comercial, cabe destacar:

Los sistemas de detección básicos o los **sistemas de detección precoz o multisensoriales**, para áreas de exposición y almacenaje de productos.

Los equipos de pulsación puntual, para casos de emergencia

- **Sistemas de detección de incendios**

Un sistema de detección de incendios lo conforma el conjunto de elementos, equipos y sistemas instalados para asegurar el conocimiento precoz de un incendio en sus inicios posibilitando una intervención rápida y eficaz.

Por tanto, la función de un sistema de detección automática de incendios es la de descubrir el foco en el tiempo más corto posible y dar la alarma para que puedan tomarse todas las medidas apropiadas, como evacuación del recinto, llamada a servicios de intervención, activación automática de los sistemas de extinción, etc.

Los componentes de los sistemas de detección automática de incendios están regulados en diversas normas tecnológicas.

Tipos de sistemas. Según su configuración y tecnología de fabricación, los sistemas de detección de incendios se clasifican:

- *Sistemas convencionales.* Distribución de los detectores en zonas, definidas mediante el tendido de cableado, en las que no es posible identificar individualmente a los detectores asociados a ellas. El recurso de indicadores de acción asociados a cada detector o grupo de ellos exige la supervisión personal como único medio de localizar exactamente el punto de alarma de incendio.
- *Sistemas direccionales.* Distribuidos en lazos, zonas y subzonas, mediante los cuales es posible identificar un número determinado de puntos de alarma de incendio.
- *Sistemas identificables.* Distribuidos en lazos o bucles, identifican el punto donde se ha producido una alarma de incendio y lo reportan a la central de incendio sin más posibilidades de actuación.
- *Sistemas analógicos.* Distribuidos en lazos o bucles, disponen de identificación puntual de la alarma y de evaluación analógica de la zona protegida. Además, permiten actuaciones como: evaluar el nivel ambiental, programar desde la central los valores en cada detector, comunicación bidireccional, mantenimiento desde la misma central, etc.

Componentes del sistema. El sistema de detección de incendios básicamente consiste en:

- Equipos que envían señales. Una serie de detectores de incendio y pulsadores manuales, distribuidos por toda la instalación, capaces de señalar la presencia de un incendio en su estado inicial.
- Equipos que reciben señales. El sistema de aviso de alarma será acústico, sirenas y/o altavoces, y permitirá la transmisión/recepción de alarmas locales y de alarma general. Asociados al sistema de detección, también reciben señales otros equipos como puertas cortafuego, exutorios de humos, repetidores, etc.
- Equipos de control. Central de detección automática donde se centralizan las alarmas y donde reside toda la lógica de funcionamiento, por la cual se llevan a cabo una serie de acciones preventivas programadas en caso de emergencia.

Los componentes más significativos de un sistema de detección de incendios son:

- Detectores de incendio.
- Centrales de incendio.

Detectores de incendio. El detector de incendio es el elemento que posee como mínimo un sensor que controla de manera continua o a intervalos regulares un fenómeno físico y/o químico asociado a un incendio, y que proporciona como mínimo una señal al equipo de control y señalización. La decisión de dar la alarma de incendio o de hacer funcionar un equipo de protección automático contra incendio puede realizarse a nivel del detector o de la central.

En función del fenómeno detectado, los detectores se clasifican en:



- Detectores de humo. Detector sensible a las partículas de los productos de combustión y/o de pirólisis en suspensión en el aire (aerosoles).

Detector de humo por ionización. Sensible a los productos de combustión capaces de afectar las corrientes de ionización en el interior del detector. Detecta tanto partículas visibles como invisibles y tanto humo negro como blanco. Es el más adecuado para la detección de incendios con humo y llamas.

Detector óptico de humos. Sensible a los productos de combustión capaces de modificar la absorción o la difusión en la zona infrarroja, visible y/o ultravioleta del espectro electromagnético. Detecta partículas visibles y de humo blanco. Es el más adecuado para la detección de incendios con mucho humo y poca llama.

- *Detectores de temperatura.* Detector sensible a un incremento de temperatura.

Detector térmico. Se activa cuando la temperatura ambiente excede de un determinado valor previamente establecido.

Detector termovelocimétrico. Se activa cuando el incremento de la temperatura excede de un cierto valor en un tiempo determinado o se llega a un valor de temperatura prefijado.

- *Detectores de llamas.* Detector sensible a la radiación emitida por las llamas procedentes de un fuego. En función del espectro de luz preferente emitido por la sustancia en combustión, los tipos básicos son:

Detector de infrarrojos (IR).

Detector ultravioleta (UV).

Detector combinado (IR+UV).

- *Detectores de gases.* Detector sensible a los productos de combustión gaseosos y/o de descomposición producidos por el calor.

En función del número de sensores que incorpora, los detectores se clasifican en:

- Unisensoriales. El detector dispone de un único sensor de acuerdo a un único principio de funcionamiento (iónico, óptico o térmico).
- Multisensoriales. El detector dispone de dos o tres sensores de acuerdo a dos o tres principios de funcionamiento (iónico+ óptico, iónico+óptico+térmico, etc.).

Existe una adecuación de aplicación de cada tipo de detector en función de determinados parámetros ambientales.

• **Centrales de incendio.** La central de incendio constituye la parte central del sistema de detección de incendios y básicamente realiza las siguientes funciones:

- Proporciona la alimentación eléctrica al resto de componentes de la instalación (detectores, pulsadores, avisadores, etc.).
- Comunica con los componentes de la instalación, indicando las situaciones de alarma, fallos, identificación de puntos, etc.
- Transmite la señal de alarma, activando los dispositivos de alarma, alerta y mando de las instalaciones.
- Vigila la instalación y avisa sobre cortocircuitos, cortes en la línea, fallos de alimentación, etc.
- Controla las señales de entrada y salida.
- Controla el funcionamiento programado, que deberá estar basado en las características, en muchos casos previsibles, del desarrollo de un posible incendio.

Igualmente, la central de incendio es el equipo que activa otros dispositivos asociados que forman parte de sistemas diferentes al de detección. A través de las salidas que posea puede telemandar:

- El sistema de evacuación de humos.

- El cierre de puertas cortafuego.
- La activación de sistemas de extinción automática.
- La activación de transmisores telefónicos de alarmas.
- El bloqueo de ascensores en planta baja.

- **Pulsadores manuales**

Los pulsadores manuales de alarma son los dispositivos de accionamiento manual que permiten provocar voluntariamente una alarma y transmitir esta señal a la central de incendio. Son un elemento esencial en toda instalación de detección de incendios.

Su ubicación será tal que la distancia máxima a recorrer, desde cualquier punto de la instalación hasta un pulsador, no supere los 15 m.

3.2.6 EXTINCIÓN AUTOMÁTICA

Una instalación fija de extinción automática detecta y extingue un incendio en sus comienzos o lo contiene de manera que se pueda realizar la extinción por medios manuales o por los servicios contra incendios.

Este tipo de instalaciones incluye un sistema de alarma, destinado a hacer patente el funcionamiento de la instalación y sus incidencias.

- **Sistemas automáticos**

El diseño, instalación y puesta en marcha deben basarse en un detallado conocimiento de la zona protegida, su uso y la organización de la alarma.

En función de las características del riesgo que se ha de proteger y las de los diferentes agentes extintores se definirá la necesidad, o no, de instalar sistemas fijos de extinción y, en caso afirmativo, qué sistemas instalar.

Las características que hay que tener en cuenta en una instalación de sistemas fijos de extinción son:

- Clasificaciones.
- Campo de aplicación.
- Consideraciones de uso.
- Especificaciones de los equipos.
- Suministro del agente extintor.
- Características y condiciones a cumplir por los equipos a instalar.
- Parámetros de diseño del sistema.
- Certificaciones de los equipos.

En el Reglamento de Instalaciones de Protección Contra Incendios se recogen las características que deben reunir los sistemas fijos de extinción posibles de instalar:

- Sistemas fijos de rociadores automáticos de agua
- Sistemas fijos de extinción por agua pulverizada
- Sistemas fijos de extinción por espuma física de baja expansión
- Sistemas fijos de extinción por polvo, sus características y especificaciones
- Sistemas fijos de extinción por agentes extintores gaseosos

Los mecanismos de disparo serán por medio de detectores de humo, elementos fusibles, termómetro de contacto, termostatos o disparo manual en lugar accesible.

La capacidad de los recipientes de gas a presión deberá ser suficiente para asegurar la extinción del incendio. Las concentraciones de aplicación se definirán en función del riesgo, debiendo quedar justificados ambos requisitos.

Estos sistemas sólo serán utilizables cuando quede garantizada la seguridad o la evacuación del personal.

Además, el mecanismo de disparo incluirá un retardo en su acción y un sistema de prealarma de forma que permita la evacuación de dichos ocupantes antes de la descarga del agente extintor.



3.2.7 CONTROL Y EMERGENCIA

Los sistemas de control y emergencia son aquéllos destinados, principalmente, a dirigir el flujo de las personas.

Entre los principales equipos, sistemas e instalaciones de aplicación a los establecimientos comerciales, podemos citar:

Los sistemas de control de rondas, para vigilancia nocturna o festiva.

Los equipos de radiocomunicaciones, para el personal de vigilancia.

Los sistemas buscapersonas, para personal directivo y de seguridad.

Las instalaciones de interfonía y de megafonía, para mensajes y consignas de seguridad.

• **Sistemas de control de rondas**

Los sistemas de control de rondas de vigilancia y protección que efectúan los vigilantes de seguridad verifican que se ha efectuado el paso obligado por un punto determinado y siguiendo un horario prefijado y programado.

El sistema de control de rondas en esencia consiste en:

- *Equipos portátiles.* Consisten básicamente en unos lectores transportables en los que se registra una señal del terminal fijo. En estos equipos quedan registrados igualmente otros datos como puedan ser la fecha, hora, número de rondas e identidad del vigilante.
- *Equipos terminales.* Son elementos fijos que se sitúan en lugares estratégicos e identifican el punto exacto en donde están situados.
- *Unidad central.* Esta unidad es un equipo en donde se vuelcan los datos obtenidos durante las rondas. Normalmente cuentan con una conexión a impresora y/u ordenador personal para gestión y control, confección de históricos, listados, etc.

Para el establecimiento de un sistema de control de rondas habrá que:

- Determinar las rutas a seguir (interiores/exteriores).
- Determinar el número de lectores.

- Determinar horarios y tipos de rutas (de control, chequeo, etc.).

• Equipos de radiocomunicaciones

Los radiocomunicadores son transceptores/receptores que operan en HF, UHF o VHF diseñados para las comunicaciones orales.

Por lo general, no permiten la explotación en duplex (comunicación bilateral y simultánea), lo que exige que el usuario conozca los procedimientos de explotación. La comunicación normalmente se realiza en semiduplex, que consiste en que se establece en los dos sentidos (emisor-receptor), pero no de forma simultánea.

Las redes de comunicación para uso profesional se basan en frecuencias asignadas por la Dirección General de Telecomunicaciones, siendo en muchos casos compartida por otros usuarios. Esto obliga a que los equipos estén dotados de un codificador/decodificador de subtonos, que mezclan con la señal voz, un tono no audible en el momento de la transmisión que sólo es detectado por el equipo que contenga este subtono. También, para evitar interferencias, se emplea un sistema de inhibición de transmisión en presencia de portadora, esto es, un equipo que no emite si detecta una portadora en la frecuencia asignada, ya que el otro equipo estará emitiendo en ese momento.

Los últimos equipos existentes en el mercado poseen un sistema de control de transmisiones que permiten a las estaciones directoras saber qué equipo emite la señal a través de unos tonos que personalizan el equipo, y así poder utilizar esta codificación de forma inversa para que la emisora seleccione con qué equipos desea comunicar.

También se han difundido las redes de grupos cerrados con asignación dinámica de canales, conocidas como red trunking, que fundamentalmente consiste en una infraestructura común de centros de control, estaciones base, repetidores, etc., que permiten que varios grupos de usuarios utilicen un sistema de comunicación compuesto por varios canales. Cuando un equipo llama y marca una serie de dígitos de identificación a su base, el sistema le asigna un canal libre estableciéndose la

comunicación entre el emisor y el receptor deseados, sin escucha por parte del resto de los usuarios.

- **Sistemas buscapersonas**

Los buscapersonas son *receptores portátiles de mensajes, vía radio, que aparecen en un display alfanumérico.*

Este sistema de comunicación para el control y casos de emergencia se basa en la utilización de un sistema alfanumérico dentro de las instalaciones del establecimiento comercial. Cuando el centro de control de seguridad recibe un aviso de una incidencia, transmite la incidencia exacta, el lugar y el procedimiento a seguir, según los planes previamente establecidos. Esto permite que la incidencia sea recibida rápidamente por un gran número de personas (normalmente el servicio de vigilancia y los empleados que intervienen en caso de emergencias).

Cuando la alarma cesa, o se ha solucionado el incidente, se envía otro mensaje a los receptores del sistema indicándoles que la situación ha vuelto a la normalidad.

Igualmente, para situaciones de emergencia es de aplicación la telefonía móvil.

- **Instalaciones de interfonía y megafonía**

Interfonía es la *difusión bidireccional o pluridireccional de sonido dentro de un determinado ámbito espacial.*

El diseño de las instalaciones de interfonía se realizará acorde con las necesidades específicas de cada organización y tipo de servicio, optimizando la eficiencia de la información del Departamento de Seguridad y de los otros servicios de emergencia.

Estos sistemas deben ser capaces de operar las 24 horas del día, incluso en caso de fallo de alguno de los equipos de la red.

Los aspectos que caracterizan estas instalaciones son:

- Versatilidad
- Privacidad
- Calidad de emisión

La megafonía es un sistema de comunicación unidireccional del sonido dirigido desde un punto central al espacio.

Las instalaciones de interfonía y megafonía, como partes integrantes de los medios activos de seguridad, cumplen **funciones de especial relevancia**, como son:

- Intercomunicar punto a punto avisos, órdenes e instrucciones de forma privada y discreta.
- Comunicar mediante mensajes hablados: órdenes e instrucciones al personal de un área, planta o todo el edificio, en caso de emergencia.
- Comunicar consignas al personal de emergencia y seguridad.

Por ello, las instalaciones de interfonía y megafonía deben estar protegidas contra la intrusión de personas no autorizadas, especialmente durante la gestión de las situaciones de emergencia.



4. RECOMENDACIONES EN MATERIA DE SEGURIDAD

4.1 RECOMENDACIONES GENERALES

- Es recomendable no esperar a sufrir un robo para adoptar medidas de seguridad. Sin embargo, hay que **adecuar** la prevención al tipo de comercio o establecimiento y debe optarse por una **selección** ponderada de los medios o medidas de seguridad lógicas.
- En función de los diferentes tipos de establecimientos comerciales, existen **diversos sistemas de seguridad** que pueden aplicarse en el interior, en el perímetro y en los accesos.
- Resulta necesario llevar a cabo un **estudio** para identificar las medidas de seguridad aconsejables y para delimitar el área de seguridad, objeto de protección, identificando los puntos débiles y suprimiendo, en la medida de lo posible, accesos secundarios.
- Las medidas de **prevención** contribuyen a mejorar de forma notable la seguridad del establecimiento y a **facilitar** las tareas posteriores de **investigación** de los delitos.
- El uso evidente y habitual de medidas de seguridad **desmotivan al** posible **delincuente** y hacen que éste se lo plantee antes de cometer el delito.
- La instalación del sistema de seguridad no es, en sí misma, suficiente. Además, es preciso que, tanto el propietario del establecimiento como los técnicos de la empresa de seguridad, lleven a cabo **comprobaciones periódicas** así como el **mantenimiento y revisión** adecuados de sus componentes, para garantizar su buen funcionamiento.
- Toda medida que implique **pérdida de tiempo para el delincuente** significa un aumento de la posibilidad de detección y de respuesta adecuada ante el delito.

- Un **técnico en seguridad** puede diseñar un proyecto de instalación o mejora del sistema adaptado a las necesidades y características de su establecimiento.
- La **señalización** adecuada mediante rótulos, tanto en accesos como en el interior del establecimiento, de la existencia de **medidas** de seguridad instaladas.
- Comprobar el grado de cobertura de la póliza de **seguros** en caso de **hurto** y en caso de **robo**, y analizar las diferencias.
- Tomar **precauciones extraordinarias** si el establecimiento funciona en horarios no habituales.
- Hay que mantener una **actitud vigilante** respecto a las **estafas**, rehuendo en general las ofertas de negocios fáciles o golosos.
- Tener a mano un listado con los teléfonos de emergencia y de las fuerzas y cuerpos de seguridad del Estado.
- Es conveniente **combinar** varios tipos de **sistemas o medidas** de seguridad.

4.2 SEGURIDAD EN EL EXTERIOR DEL LOCAL

4.2.1 PUNTOS DE ACCESO AL LOCAL

- Se ha de valorar la posibilidad de **contratar** un **servicio de vigilantes** de seguridad. En caso contrario, **designar** algún **empleado** de confianza para que se responsabilice de ello.
- Si es posible, es aconsejable instalar un **timbre** y un **sistema de control de apertura** de la puerta de acceso al establecimiento, ya sea un llamador o un sistema de apertura remota.



- Con respecto a los **escaparates**, adoptar las **medidas de seguridad** físicas y/o electrónicas que se crean necesarias para su establecimiento a fin de protegerlos (pilones antialunizaje, cristales reforzados o de seguridad, detectores de vibraciones, etc.).
- En esta línea, los escaparates deben estar dotados de **películas fílmicas anti-rotura** que eviten tanto accesos no deseados, como accidentes.
- También los escaparates deben mantenerse **despejados** para que no impidan observar el exterior desde el interior y viceversa.
- Igualmente, las **ventanas** deben estar **libres de obstáculos** para permitir una buena visión desde el exterior.
- Puede ser conveniente instalar **rejās** y/o **persianas** antipalanca y anticorte en puertas, ventanas y otros accesos del establecimiento (respiraderos, conductos de ventilación, tragaluces, aberturas de los sόtanos, etc.). Las persianas no deben ser macizas para permitir la visualización del interior cuando estén echadas.
- Es necesario instalar **cerraduras de seguridad** en puertas, ventanas y otros accesos al establecimiento y reforzar los marcos y las bisagras.
- En caso de **pérdida de llaves**, cambiar la cerradura inmediatamente. Hacer lo mismo con los mandos a distancia que abren la persiana, desactivan la alarma, etc.
- Hay que tener en cuenta que los **andamios de las obras** pueden facilitar el acceso a los establecimientos.
- Una **iluminación** adecuada da seguridad en los accesos, en el exterior y en las zonas que deben protegerse más.
- Comprobar el estado de deterioro y dilatación de los **marcos de puertas y ventanas**.
- Instalar medidas de **protección anti-intrusión** en conductos de ventilación, respiradores o aberturas del sόtano.

- No descuidar los **accesos secundarios** del negocio.
- Las **puertas** deben ir **dotadas** de cerraduras anti-atacos, bulones de seguridad y, si es posible, barras metálicas interiores que eviten los apalancamientos.
- Si las **puertas** son de **vidrio**, deben fijarse a la base y es recomendable dotarlas de plásticos de protección anti-vandalismo.
- Prestar atención a la parte **exterior** del local y cuidar que no haya **marcas** exteriores. Algunos delincuentes marcan los locales en el exterior y luego realizan butrones sobre los locales marcados.
- Tener especial cuidado con la seguridad del **almacén**, sobre todo en determinados momentos del año con sobre stock (verano o navidades).

4.2.2 APERTURA Y CIERRE

- Según la naturaleza del negocio puede ser recomendable tomar medidas de seguridad **desde la salida del domicilio**. Comprobar que no haya movimientos sospechosos, o desconocidos con conductas extrañas, y en caso de duda ponerse en contacto con la Policía.
- Hay que procurar que la persona que abra o cierre el establecimiento comercial esté **acompañada**.
- En el cierre, dejar la **caja registradora** vacía y visiblemente abierta para evitar que la fuerquen en caso de robo.
- Evitar crear **posibles escondites** por almacenamiento de material y comprobar siempre que todas las **instalaciones** han quedado **vacías** (cuartos,



baños, armarios, etc.).

- Asegurar siempre de que **puertas y ventanas** queden cerradas y el sistema de **alarma** conectado.

4.2.3 ALARMAS EXTERIORES

Una buena forma de evitar robos en su negocio es contar con un sistema de alarma conectado a una Central Receptora de Alarmas.

El **funcionamiento** de las alarmas es posible dividirlo en cuatro **fases**:

1. Disuasión: la simple presencia de la placa indica a cualquier intruso que su negocio cuenta con un sistema de alarma, lo que puede traducirse en un aviso inmediato a las Fuerzas y Cuerpos de Seguridad del Estado en caso de intento de intrusión.
2. Detección: los detectores volumétricos se activan si registran movimiento y/o aumento de temperatura. Cualquier intento de intrusión hará que la señal de alarma llegue a la Central Receptora.
3. Recepción: las alarmas están conectadas a una Central Receptora. Cuando ocurre algo, los profesionales de la empresa de seguridad contratada contactan al instante para comprobar si se trata de una falsa alarma. De no ser así, proceden a llamar de inmediato a la Policía.
4. Intervención: es posible contratar con las empresas de seguridad un servicio de intervención inmediata, mediante el cual al activarse la alarma de su local le envían un vigilante motorizado.

Así, se puede decir que:

- La instalación de un **sistema de alarma sonora** adecuado al establecimiento y conectado a una central receptora de alarmas con una línea telefónica protegida, no visible y separada del resto de líneas es una medida de seguridad de gran importancia.

- **Consultar** con **empresas autorizadas** por la Dirección General de Policía que pueden asesorar sobre qué sistema instalar en el local de negocio.
- Es recomendable instalar un **sistema de alarma mixto** contra personas intrusas e incendios.
- **Comprobar** de vez en cuando su **funcionamiento**.
- En esta línea es conveniente **revisar** periódicamente los **detectores volumétricos** del sistema de alarma. Los delincuentes, en horario comercial y con el establecimiento abierto al público, colocan de forma discreta, una lámina de plástico transparente encima de los detectores, difícil de detectar a simple vista. Esto hace que los detectores no funcionen correctamente y que los delincuentes puedan aprovechar el horario de cierre del establecimiento para acceder sin ser detectados por el sistema de alarma. En estos casos no hay que tocar nada ni comentarlo con nadie y se debe avisar a los agentes de seguridad.
- **Anunciar** de forma bien visible que su establecimiento está protegido por un sistema de alarma.
- Asegurarse de que el **personal** conoce el sistema para eliminar los riesgos de falsas alarmas.
- **Notificar** un **teléfono** de contacto o el de la empresa instaladora a la Policía para que puedan avisar en caso de que suene la alarma.

4.2.4 VIDEOVIGILANCIA EXTERIOR

La videovigilancia exterior conlleva el uso de cámaras con acceso a la vía pública. Se debe de recordar que la legitimación para el uso de instalaciones de videovigilancia se ciñe a la protección de entornos privados. La prevención del delito y la garantía de la seguridad en las vías públicas corresponden en exclusiva a las Fuerzas y Cuerpos de Seguridad del Estado. Por tanto la regla general es la prohibición de captar imágenes de la calle desde instalaciones privadas.

No obstante, en algunas ocasiones la protección de los espacios privados sólo es posible si las cámaras se ubican en espacios como las fachadas.

A veces también resulta necesario captar los accesos, puertas o entradas, de modo que aunque la cámara se



encuentre en el interior del edificio, resulta imposible no registrar parte de lo que sucede en la porción de vía pública que inevitablemente se capta. Por todo ello el artículo 4.3 de la 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, dispone:

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.

Para que esta excepción resulte aplicable, no deberá existir una posibilidad de instalación alternativa. Debe tenerse en cuenta que:

- La utilización de instalaciones de videovigilancia en la vía pública **se reserva a las Fuerzas y Cuerpos de Seguridad** por 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 del Estado en lugares públicos.
- El artículo 4.3 de la Instrucción 1/2006 **no** constituye una **habilitación** para captar imágenes en espacios públicos.
- El responsable del fichero adecuará el uso de la instalación de modo que el **impacto en los derechos** de los viandantes sea el **mínimo** posible.

- **En ningún caso se admitirá** el uso de prácticas de **vigilancia más allá del entorno objeto de la instalación** y en particular en lo que se refiere a los espacios públicos circundantes, edificios contiguos y vehículos distintos de los que accedan al espacio vigilado.
- La **señalización** garantizará en todo caso los derechos de los afectados.
- Las **indicaciones** de uso y seguridad facilitados **al personal** contendrán de modo expreso instrucciones específicas que garanticen un uso adecuado y proporcional de los recursos.

4.2.5 INGRESOS DE EFECTIVO EN ENTIDADES FINANCIERAS

- La persona que realice los ingresos debe de proceder siempre con la mayor **reserva** posible. Evitar compartir información sobre estos movimientos.
- Escoger una **oficina** bancaria **próxima** al establecimiento.
- Variar la **ruta** de acercamiento a la oficina de la entidad financiera procurando ir por vías concurridas.
- También es conveniente no realizarlos siempre el mismo **día** a la misma **hora**. Hay que **evitar rutinas** y se debe ir variando para que los delincuentes no dispongan de pautas a seguir para cometer el delito.
- En caso de hacer el **traslado en coche**, cuidar de que esté siempre en buenas condiciones y con el depósito suficiente, evitar hacer paradas dejando el dinero en el vehículo y llevar éste, en un lugar que no sea accesible desde la ventanilla.
- Cuando se trasladen grandes sumas de dinero encima evitar, en la medida de lo posible, el **trato con desconocidos**.
- Durante el trayecto **mantenerse alerta** para detectar la presencia de posibles delincuentes que observen o tengan una actitud sospechosa.
- Si se sospecha de que puedan **estar siguiendo**, dirigirse a una comisaría o a

un Policía.

- **Evitar llevar mucho dinero** en una única entrega a las entidades bancarias. Es preferible efectuar varios ingresos para evitar llevar la totalidad de la recaudación.
- No llevar el dinero en bolsas de mano o bandoleras colgadas del hombro. Se deben llevar en **bolsillos interiores** de la ropa. De esta manera evitaremos tirones.
- Considerar la posibilidad de **contratar** el **servicio** de alguna empresa de seguridad para realizar la recogida de la recaudación comercial.

4.2.6 RELACIONES CON OTROS AGENTES

- **Establecer relaciones** con los agentes de las Fuerzas y Cuerpos de Seguridad del entorno, así como con los vecinos y demás comerciantes. Las medidas de seguridad tomadas en conjunto aumentan la efectividad de las medidas individuales.
- **Participar** en **asociaciones de comerciantes** del sector o territorio es una manera de enfrentarse en grupo a los posibles problemas y establecer soluciones y medidas de seguridad coordinadas.

4.3 SEGURIDAD EN EL INTERIOR DEL LOCAL

4.3.1 CAJAS REGISTRADORAS

- **Ubicar** la caja registradora separada, o protegida por el mostrador, en el lugar que se elija y se considere visible desde cualquier posición del local.

- Intentar **no acumular** demasiado **efectivo** en la caja registradora. Utilizar sólo el efectivo necesario para las transacciones comerciales diarias. Fijar una cantidad e ir retirando el exceso reservando lo necesario para garantizar el cambio.



- Este **dinero** retirado de la caja registradora se debe de **ingresar** regularmente en una entidad financiera o caja de seguridad.
- Cuando se **retire dinero** de la caja registradora, cerrar la puerta de acceso al establecimiento. Realizar esta acción en diferentes horas de manera aleatoria.
- No esperar a **cerrar la caja** a última hora, antes del cierre del establecimiento. La persona que lo haga es conveniente que se encuentre acompañada y en un lugar donde el público no pueda verlo.
- La caja registradora debe estar **iluminada** y ser fácilmente **visible** desde el exterior. Antes de cerrar, dejarla **abierta** y **vacía** para evitar destrozos inútiles.
- Al disponer de **cámaras** de seguridad, comprueba que al menos una siempre esté grabando la posición de la caja registradora.

4.3.2 BILLETES DE EURO

Los billetes de euro incorporan muchos **elementos de seguridad** de una gran complejidad técnica que siguen normas internacionales muy estrictas en cuestión de seguridad.

- **Comprobar** siempre las diferentes medidas de seguridad y particularidades que presentan los billetes de euro (impresión calcográfica, marca de agua, hilo de seguridad, etc.). En caso de duda, es conveniente tocar, mirar, inclinar o girar el billete para verificar su autenticidad



- (según una recomendación del Banco Central Europeo).
- Es recomendable disponer de **detectores de billetes falsos** y/o de otros medios o dispositivos similares. El mayor número de billetes falsos corresponde a los de 50 €.
- Si se cree que un billete es falso, **no aceptar, retener y avisar** a los servicios de seguridad (seguridad privada o Policía). Evitar en cualquier caso el enfrentamiento con la persona, evitando riesgos y discusiones, informando de que el billete aparentemente podría ser falso y que puede haber sido víctima de una estafa.
- En caso de que la **persona quiera irse** del establecimiento sin esperar la llegada de los servicios de seguridad, no oponerse. Hay que fijarse en los rasgos característicos, ropa y detalles de la persona (descripción física, tatuajes, cicatrices, etc.) y de los acompañantes y/o vehículos para facilitarlos posteriormente a las fuerzas y cuerpos de seguridad.
- Si a pesar de todas las precauciones adoptadas se confirma que se ha recibido un billete falso, hay que **ponerlo en conocimiento de la Policía**, presentando una denuncia o entregándolo en comisaría. De esta forma, la unidad de falsificación de moneda de las fuerzas y cuerpos de seguridad del Estado, encargada de perseguir estos delitos, tendrá conocimiento de ello.
- **En ningún caso** hay que **desprenderse del billete** intentando pagar con él,

ya que, en función del valor del billete, se podría incurrir en un delito (si excede de 400 €) o falta penal (si es igual o no excede de 400 €).

4.3.3 CAJAS FUERTES

- Tener en cuenta que puede ser más efectivo **ir ingresando** el **dinero** en un banco o caja o disponer de un servicio de recogida de efectivo. Nunca acumular grandes sumas de dinero en el negocio.
- En caso de poseer una caja fuerte, **esconderla** puede suponer que los ladrones causen **daños buscándola**.
- Si la caja fuerte ha de estar **fija**, empotrar la caja fuerte en el suelo.
- **Modificar** la **combinación** de la caja fuerte cuando se produzcan cambios en su plantilla de trabajadores.

4.3.4 VIDEOVIGILANCIA INTERIOR

- Es recomendable la instalación de un **sistema de video vigilancia** proporcional al establecimiento, con cámaras visibles (disuasorias) o camufladas, con grabación de imágenes.
- Las cámaras deben **enfocar** al acceso del establecimiento y al lugar donde se encuentra la caja registradora.
- La **grabación de las imágenes** debe hacerse en un disco duro no localizable, ni desde el exterior ni vía Internet. Este disco duro debería estar fuera del alcance de los posibles delincuentes, para evitar que se puedan llevar la grabación de las imágenes.
- Se debe **conservar** estas **imágenes** durante un período razonable de tiempo
- Evaluar la posibilidad de colocar **cámaras** de seguridad **ficticias**.

CÁMARAS CONECTADAS A INTERNET

Cada vez resulta más frecuente el uso de videocámaras IP y Webcams capaces de transmitir datos en formato digital a través de Internet. La tecnología permite el ahorro de costes al facilitar la grabación directa en soporte digital y facilita el nacimiento de nuevos servicios de videovigilancia.

A diferencia de las tradicionales, la cámara IP se conecta a Internet directamente como cualquier ordenador conectado a la red. Por ello la visión de las imágenes captadas por la cámara puede realizarse desde cualquier ordenador conectado a Internet, a través del navegador habitual, sin más que introducir la dirección IP de la cámara.

Se trata de productos muy publicitados, fácilmente adquiribles y que no suelen requerir de conocimientos técnicos especiales para su instalación, pero respecto de cuyo uso deben analizarse los riesgos.

- El uso de tales cámaras comporta **riesgos adicionales** cuando no se configura adecuadamente el uso del programa y/o el entorno de comunicaciones.
- La **configuración por defecto** del software puede no reunir las garantías de seguridad facilitando el acceso abierto a las imágenes por cualquiera. Se deben de revisar si las funciones de identificación y autenticación se encuentran activadas con el fin de evitar accesos de terceros a las imágenes y de garantizar que sólo acceden los usuarios autorizados.
- Asimismo, la grabación digital permite un **uso fácil de las imágenes**.

Por ello no debe de olvidarse que:

- Es irrelevante el medio técnico empleado. La instalación de cualquier sistema de videovigilancia con fines de seguridad **requiere la participación** de una **empresa de seguridad** debidamente autorizada por el Ministerio del Interior.
- El sistema deberá cumplir con el nivel de seguridad que corresponda conforme al Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de **Protección de Datos** de Carácter Personal (RDLOPD), aprobado por el

Real Decreto 1720/2007, de 21 de diciembre y en particular:

- Se contará con procedimientos de **identificación y autenticación de los usuarios** del sistema y no se permitirá el acceso de terceros no autorizados.
- Se garantizará la **seguridad en el acceso** a través de redes públicas de comunicaciones.
- Se tendrá en cuenta la naturaleza de la instalación al definir las **obligaciones del personal**.



4.3.5 ILUMINACIÓN INTERIOR

- Una **correcta** visibilidad de todos los espacios del negocio, y una buena iluminación tanto en el interior como en el exterior, es la mejor manera de evitar hurtos.
- Mantener iluminado el interior del negocio en las **horas de cierre**.

- Procurar sustituir las bombillas y neones tradicionales por **lámparas de bajo consumo**. Se reducirá el gasto de electricidad y se evitarán incendios ya que estos sistemas de iluminación no se calientan tanto como los convencionales.
- Así, como las luces constituyen importantes focos de calor, **no dejar en sus proximidades** ropas, papeles u otros elementos combustibles.
- Extremar las precauciones en las **instalaciones temporales de los escaparates**.
- **No sobrecargar** las instalaciones eléctricas.
- **Mantener en buenas condiciones** el cableado y los empalmes eléctricos.
- No descuidar la iluminación de los **accesos secundarios, salidas de emergencia y patios traseros**.

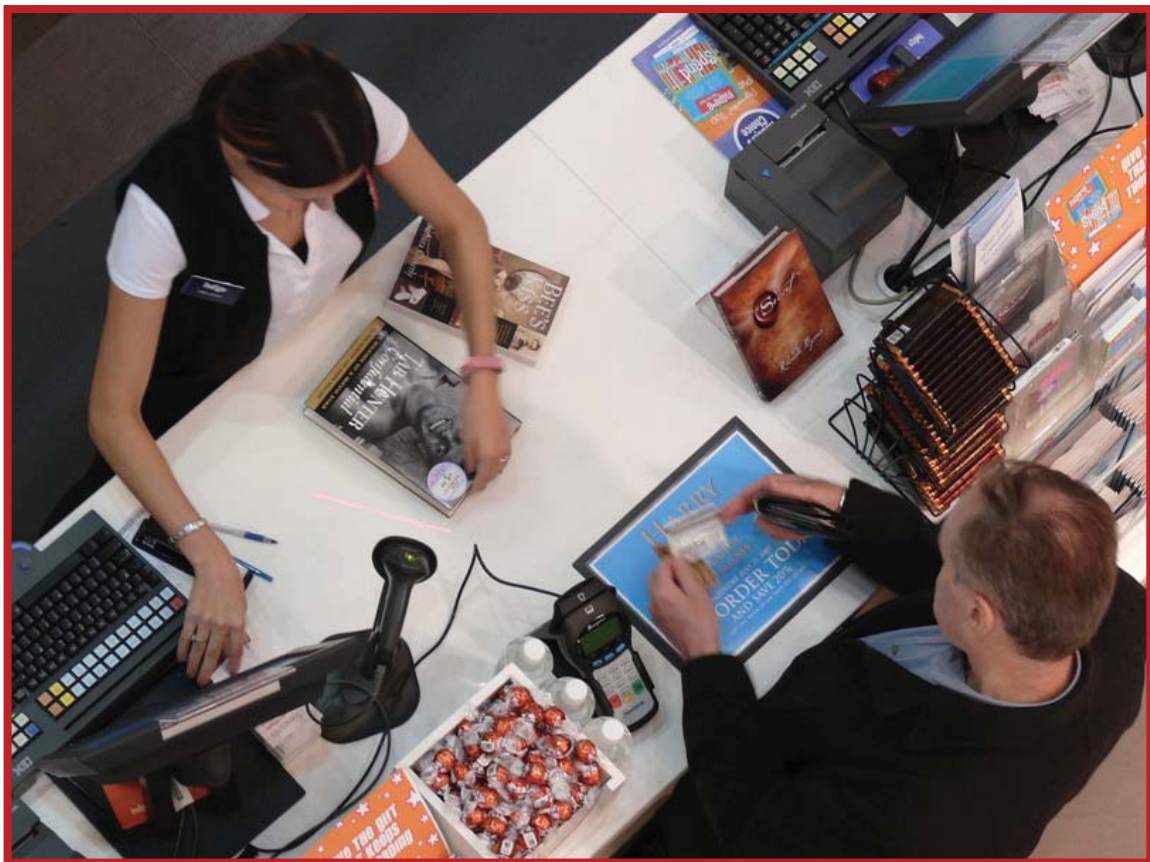
4.3.6 PRODUCTOS COMERCIALIZADOS

- Es recomendable instalar **sistemas de protección** mecánicos o electrónicos en los artículos que están en venta.
- Los **objetos pequeños**, pero de valor económico elevado, deben exhibirse dentro de escaparates o vitrinas cerradas con llave y ésta debe estar en todo momento en posesión del personal del establecimiento.
- En caso de tener **objetos** expuestos **en funcionamiento**, por ejemplo ordenadores portátiles o teléfonos móviles, atarlos con un cable de acero o similar a la mesa o expositor.
- Evitar concentrar **objetos de gran valor** en una misma zona y mantenerlos fuera del alcance del público. Tampoco situarlos cerca de los accesos del establecimiento.
- Si es viable, exponer cara al público el **embalaje del producto vacío**.

- A veces la distribución de los artículos según estrategias de **merchandising** no coincide con la distribución según estrategias de **seguridad**. Habría que encontrar un **equilibrio** entre ambos aspectos.
- Las **vitrinas y expositores** del establecimiento deben estar cerrados con llave. La llave no debe dejarse puesta en la cerradura.

4.3.7 CLIENTES Y EMPLEADOS

- **No** se debe **informar** a personas desconocidas sobre los sistemas de seguridad adoptados en el establecimiento.
- **Llamar a los agentes** de seguridad en el caso de observar la presencia de alguna persona sospechosa en las inmediaciones del establecimiento.



CLIENTES

- En el establecimiento, se debe **delimitar** claramente las **zonas** de venta, a las que el público tiene libre acceso, y las zonas privadas, donde está restringido el paso de personas ajenas al establecimiento.
- Cuando se **enseñe** a un cliente **objetos** de valor, se deben de guardar antes de enseñar el siguiente. Determinados objetos pueden ponerse en exposición en embalajes vacíos.
- **Observar** posibles **comportamientos sospechosos** entre los clientes y curiosos (nerviosismo, movimientos extraños, etc.). Así, observar si hay personas que permanecen en actitud vigilante o que toman nota de movimientos del personal de ventas. Hacer lo mismo con personas que entren en el comercio curioseando, haciendo preguntas y sin muchas intenciones de comprar.
- Desconfiar de las personas que entren en el establecimiento **con un casco de moto** puesto, ya que se trata de una práctica habitual para cometer robos en establecimientos comerciales en áreas metropolitanas.
- También se debe de estar alerta cuando **entren** en el establecimiento **grupos numerosos**. Éstos pueden actuar de forma coordinada para cometer delitos.
- Igualmente, prestar especial atención cuando el establecimiento se encuentre **lleno de clientes**, ya que los delincuentes aprovechan esta situación para cometer hurtos.
- **Asegurarse** de que **no ha quedado nadie** ajeno al establecimiento en su interior (armarios, lavabos, almacén, oficina, etc.) antes de cerrarlo, tanto al mediodía como por la noche.
- **No dejar** sus **objetos personales** (bolso, móvil, etc.) **al alcance** del público,



como por ejemplo sobre el mostrador, en una silla detrás del mostrador, en la estantería, etc.

- Advertir con rótulos, en la entrada del establecimiento, que **puede pedirse** al cliente que muestre su **bolsa de mano** (al personal de seguridad) o que lo deje en la **consigna**.

EMPLEADOS

- Es necesario que los empleados del establecimiento **conozcan** el ámbito de seguridad que les corresponde, **en función de su grado de responsabilidad**, y que sean conscientes de la necesidad de las medidas de seguridad adoptadas.
- Así, es posible **implicar** a los empleados en la seguridad del negocio con información, facilitándoles el conocimiento para el correcto uso de los sistemas de seguridad y estableciendo protocolos de seguridad (movimiento de efectivo, cierre del establecimiento, etc.).
- Concienciar a todo el personal sobre la necesidad de estar alerta.
- Recuerda a los empleados que es obligatorio comprobar el **DNI** en los **pagos con tarjeta**.
- También, un correcto conocimiento por todo el personal de los sistemas de seguridad **reducirá** el riesgo de sufrir **falsas alarmas**.
- **Modificar** la **combinación** de cajas de seguridad, ordenadores y sistemas de alarma cuando existan bajas de trabajadores.
- Establezca un código de comunicación de **palabras clave** entre los trabajadores del establecimiento para comunicarse cualquier incidente, por ejemplo en caso de robo.

4.4 SEGURIDAD Y NUEVAS TECNOLOGÍAS

4.4.1 TARJETAS DE CRÉDITO Y DÉBITO

- Hay que **controlar** rigurosamente las ventas con tarjetas, para evitar el uso de tarjetas sustraídas o duplicadas.
- Se debe de recordar que las tarjetas son de **uso personal e intransferible**.
- Hay que sospechar de **personas** con un aspecto físico que nos pueda hacer pensar en un **intento de camuflar su imagen**. Estas personas conocen la existencia de sistemas de seguridad con cámaras e intentan evitar su identificación.
- Se debe desconfiar de las **compras** compulsivas o muy abundantes donde sólo se prima el valor de los objetos y no sus características, así como de las compras importantes en días sucesivos.
- Asegurarse de que la tarjeta **no haya caducado** y que esté **firmada** por su titular. Desconfiar si se detecta manipulaciones en la zona de la firma.
- El titular está obligado a **identificarse**.
- Debe pedirse al comprador que extraiga el **documento acreditativo** de la cartera, tarjetero o monedero para poder hacer la comprobación con el documento en la mano, de manera correcta y sin dudas.
- Se debe **comprobar** siempre la fotografía, la firma y la identidad del titular con el DNI, carné de conducir o pasaporte y compararlos con la persona que facilita la documentación.



- En caso de que una tarjeta ya comprobada no permita realizar la operación de compra, el comprador **puede facilitar otra**. Entonces habrá que volver a comprobar los datos.
- **En caso de duda** sobre la legalidad de la tarjeta, no efectuar la operación y, si es posible, avisar discretamente al servicio de seguridad o a los agentes de seguridad.
- Se debe de **evitar** en todo momento la **confrontación** con la persona.

4.4.2 INTERNET

- La estafa más común en internet es el **Phishing**: consiste en un reclamo de los datos bancarios y claves vía mail o a través de una falsa web.
- Es importante recordar que ni los bancos, ni las webs de compra-venta, van a solicitar esta información **por email**.
- Cuando se vaya a entrar en la **web de un banco** o caja, desconfiar si se encuentran grandes cambios en el diseño, falta de información o errores ortográficos.
- **No entrar en estas páginas** desde vínculos recibidos por correo electrónico, desde páginas no seguras u ordenadores desconocidos y cambiar regularmente los códigos de seguridad.
- No aceptar **contratos** en internet **para recibir dinero**.
- En caso de usar servicios de **subastas** por internet se debe de saber que son más fiables las páginas que más tiempo llevan prestando sus servicios.
- El pago más recomendable en internet es el de tipo **PayPal**.
- Nunca adelantar dinero para cobrar una **herencia** de alguien que no se conozca o una **lotería** a la que no se haya jugado.

VIRUS, GUSANOS Y ATAQUES DE INGENIERÍA SOCIAL

- No instalar software que no proceda de una fuente fiable. Utilizar los servicios de descarga del fabricante o los sitios autorizados por él para la obtención de nuevas versiones o actualizaciones.
- Utilizar programas antivirus, y, si se dispone de ellos, instalar cortafuegos y programas especializados en el control de "*spyware*" y sus variedades.
- Consultar de forma periódica los sitios web con información sobre la aparición de nuevas variantes y formas de prevención.
- Realizar periódicamente copias de seguridad del contenido de los equipos informáticos.
- Tener en cuenta que una entidad financiera o prestador de servicios no va a solicitar nunca información sobre el identificador de usuario y palabras de paso. Rechazar los mensajes de correo que así se lo soliciten, los que no estén redactados en su idioma habitual de comunicación con la entidad, o los que no sean remitidos por la entidad.
- Si la entidad puede proporcionarlos, adoptar sistemas adicionales de control de acceso a sitios web con información sensible, como puedan ser tarjetas de coordenadas o dispositivos de generación de claves de acceso. Cuantos más niveles de seguridad se disponga para el acceso, más difícil será para un atacante poner en compromiso sus bienes.
- Actuar con prevención frente a ofertas económicas que ofrezcan grandes beneficios en poco tiempo y con poco esfuerzo. Pueden llevar, de aceptarlas, a la participación involuntaria en actividades delictivas.
- Ante cualquier duda, consultar al servicio de atención al cliente de la entidad o proveedor de servicios. Si ha sido objeto de un ataque, y se ha proporcionado información, comunicarlo igualmente a los servicios pertinentes de las fuerzas y cuerpos de seguridad.

BANCA Y COMERCIO ELECTRÓNICO

- Navegar por portales conocidos.
- Siempre que sea posible, utilizar certificados digitales como medio para acreditar la identidad.
- Asegurarse de que se realizan los trámites desde un equipo libre de software malicioso.
- Comprobar que la dirección que figura en el navegador corresponde con el portal de la entidad a la que se quiere acceder.
- Nunca aportar datos personales, identificadores de usuario ni contraseñas si no se ha establecido una conexión segura entre el navegador y el servidor al que se accede.
- Verificar que el certificado del sitio web con el que se ha establecido la conexión segura ha sido emitido para la entidad a la que nos conectamos y por una Autoridad de Certificación que nos ofrezca confianza.
- Desconfiar de cualquier correo electrónico que solicite identificación de usuario, contraseña o firma electrónica.
- Poner este hecho en conocimiento de los responsables del portal.
- En los sistemas de autenticación de usuario basado en contraseñas no utilizar las mismas contraseñas en los sistemas de alta seguridad que en los de baja seguridad.
- En caso de que se utilicen certificados digitales tener en cuenta que el titular de éstos es el responsable de su custodia y conservación. En ningún caso se deberá comunicar a un tercero la contraseña que permite activar la clave privada de firma. Solicitar inmediatamente a la Autoridad de Certificación la



revocación de un certificado en caso de tener conocimiento o sospecha de compromiso de la clave privada. Es muy recomendable estar bien informado del documento de la "*Declaración de Prácticas de Certificación*" emitido por la Autoridad de Certificación.

- Nunca dejar desatendido el ordenador mientras se está conectado y se ha establecido una conexión segura. Utilizar protectores de pantalla con contraseña o activar las funciones de bloqueo del terminal.
- En caso de utilizar certificados digitales almacenados en una tarjeta criptográfica no dejar ésta conectada al lector del ordenador. Cuando no sea necesario utilizar los certificados extraer la tarjeta aunque se continúe utilizando los servicios del portal.
- Introducir datos financieros sólo en sitios web seguros. Además, el acceso a dichas páginas debe hacerse tecleando directamente la dirección de la banca electrónica en la barra de dirección del navegador.
- Utilizar para las compras una tarjeta de crédito específica para estos fines, con límite de gasto reducido.

4.4.3 PROTECCIÓN DE DATOS

CORREO ELECTRÓNICO

- Hay que ser consciente de que cuando envía mensajes de correo a una variedad de **destinatarios**, se está **revelando las direcciones** de correo electrónico de los mismos que figuran en los campos "*Destinatario*" o "*Con Copia (CC)*" a todos los receptores del mensaje. Para evitarlo, se puede incluir los destinatarios del mensaje en el campo "*Con Copia Oculta (CCO)*" de tal forma que ninguno de los receptores podrá acceder a la dirección de correo electrónico del resto de los destinatarios.

- Configurar el programa de correo en el **nivel de seguridad máximo**. Si se es usuario de correo web, decantarse de ser posible por un proveedor de servicios que ofrezca análisis del contenido de los mensajes. Además, configurar el navegador en el máximo nivel de seguridad posible.
- **Mantener actualizado** el programa cliente de correo electrónico, el navegador y el sistema operativo.
- No abrir los mensajes que le ofrezcan **dudas** en cuanto a su **origen** o posible **contenido** sin asegurarse, al menos, que han sido analizados por el software antivirus.
- Activar los **filtros de correo no deseado** del programa de correo electrónico.
- Si se va a enviar por Internet documentos privados, es conveniente utilizar sistemas que permitan el **cifrado** de su contenido.

EMPLEADOS

Se trata la protección de datos con respecto a los trabajadores de los establecimientos comerciales en dos momentos diferenciados:

- Procedimiento de selección de personal
- Desarrollo de la prestación laboral

Procedimiento de selección de personal

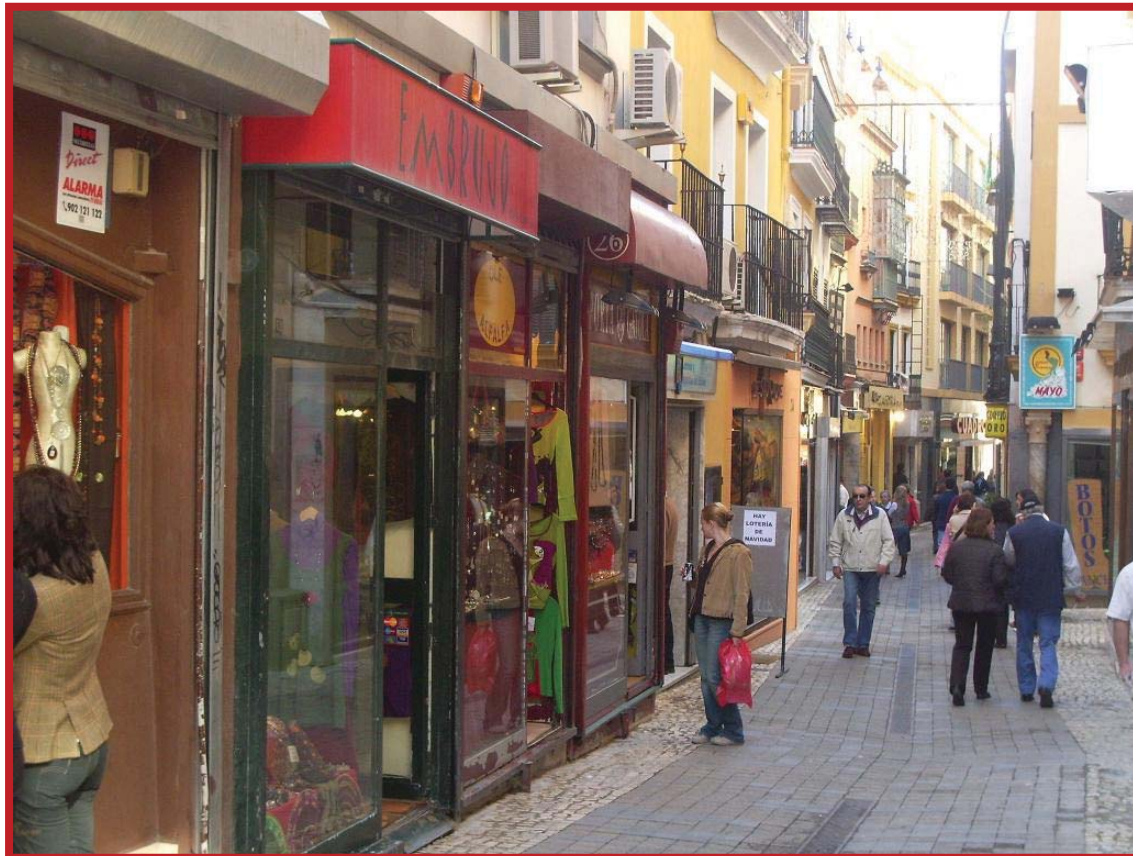
El primer tratamiento de datos personales puede producirse cuando el futuro trabajador sea un simple candidato a un puesto. Para ello deben tenerse en cuenta algunas cautelas:

- Es conveniente, cuando los recursos lo permitan, disponer de impresos de modelos de impresos tipo para la formalización del currículum y de un procedimiento de formalización y entrega de los mismos por los candidatos, ya

que ello permite no sólo informar adecuadamente sino definir con precisión el tipo de datos a tratar, establecer las medidas de seguridad etc.

- Si el currículum se presenta directamente por el candidato sin habersele solicitado deben fijarse procedimientos de información que supongan algún acuse o confirmación de conocer las condiciones en las que se desarrollará el tratamiento.

Ej. Si el currículum se remitió por correo postal o electrónico y se cuenta con una dirección electrónica facilitada por el propio interesado puede remitírsele información por ese medio solicitando confirmación de la recepción y condicionando el tratamiento de los datos al acuse de recibo. Si se presentó en un mostrador u oficina de atención debería ser informado allí por cualquier medio que acredite el cumplimiento de este deber como por ejemplo carteles, documentos de acuse de recibo y en general cualquier medio que garantice y permita probar el cumplimiento del deber de información



Desarrollo de la prestación laboral

Las relaciones laborales son dinámicas y pueden estar sujetas a cambios sobrevenidos tanto desde el punto de vista del trabajador como desde la perspectiva de la empresa. Por ejemplo, la empresa puede instalar un nuevo sistema de control de presencia basado en el uso de instalaciones de videovigilancia. Por ello, será necesario informar al trabajador en todos aquellos casos en los que se produzcan cambios que afecten al tratamiento de los datos.

4.5 DURANTE Y DESPUÉS DEL HECHO DELICTIVO

4.5.1 DURANTE EL HECHO DELICTIVO

- Ante un delito, la seguridad de las personas es lo primero. **No asumir riesgos** y conservar la calma.
- **Avisar** lo antes posible a las **autoridades**. En caso de duda, es preferible llamar a la Policía y seguir sus instrucciones, a no hacer nada por querer evitar dar un falso aviso.
- Hay que tomar **medidas de autoprotección** de forma rápida y discreta, como por ejemplo cerrar el acceso principal ante un posible intento de acceso al interior del establecimiento por parte de una persona sospechosa, simular que se está efectuando una llamada informando del hecho, etc.
- Intentar **mantener** una **distancia** prudencial con el agresor, no señalarlo ni mantener actitudes agresivas y evitar, en general, el trato directo con él. La prioridad siempre es evitar el enfrentamiento. No enfrentarse nunca al delincuente, especialmente cuando éste se encuentre armado.
- Es importante **recopilar y recordar el máximo de rasgos** característicos, apariencia física, ropa y detalles de la persona o personas (estatura y complexión, señas particulares, nacionalidad, vestimenta, vehículo, armas u objetos utilizados, etc.) que han accedido al establecimiento para poderlas facilitar, posteriormente, a la Policía. Anotar los datos puede ayudarnos.

4.5.2 DESPUÉS DEL HECHO DELICTIVO

- **Avisar** inmediatamente a los agentes de seguridad a través del 112 (Número Europeo de Emergencias), 091 (Cuerpo Nacional de Policía) ó 062 (Guardia Civil) y esperar su llegada.
- Hay que tomar las **medidas convenientes antes de acceder** al establecimiento, ya que no es recomendable acceder al interior para comprobar los hechos, dado que todavía podría encontrarse alguna persona ajena al establecimiento.
- Si en el momento del hecho delictivo había algún **testigo**, hay que pedirle sus datos y un teléfono de contacto para que la Policía lo pueda localizar para ampliar los datos sobre lo ocurrido.

- Se debe **poner** una **denuncia** inmediatamente sobre lo sucedido.



- En línea con lo que se ha dicho anteriormente, hay que facilitar el mayor número de **datos** del **suceso** y del presunto **autor**, así como la dirección y el modo de huida empleado (vehículo, a pie, transporte público, etc.). Algunos ejemplos de datos a facilitar serían la descripción de la persona, ropa que llevaba, cicatrices, tatuajes, u otras marcas características, acento del habla, posible procedencia, apariencia física o nacionalidad, si se ha hecho uso de armas, etc. Otro dato muy importante a facilitar es si los autores han pronunciado alguna palabra, mote o nombre propio en el curso del robo, que pueda conducir a su identificación.
- También hay que intentar proporcionar toda la **información** posible sobre los **objetos robados** a la Policía (inventario, facturas, números de serie,

imágenes, etc.).

- En caso de **sustracción de teléfonos móviles**, se debe entregar a la Policía los listados de llamadas realizadas a partir de la sustracción del aparato. Eso permite relacionar los teléfonos destinatarios con personas del entorno del presunto autor del delito.
- Siempre hay que informar a la Policía del incidente aunque el **delito no** se haya consumado. De esta manera se pueden evitar otros delitos.

FORMALIZACIÓN DE LA DENUNCIA

Las denuncias deben formalizarse en la Comisaría del Cuerpo Nacional de Policía o Puesto de la Guardia Civil según corresponda a la localidad donde se haya producido el hecho delictivo.

Se pueden presentar denuncias a la Dirección General de la Policía y de la Guardia Civil de diversas formas:

- Por teléfono: Marcando el **902 102 112** (Teléfono de denuncias del Cuerpo Nacional de Policía)
- Por Internet: En la Oficina Virtual de Denuncias del Cuerpo Nacional de Policía

<http://www.policia.es>

No puede denunciarse por este sistema ningún hecho en el que haya tenido lugar violencia física en las personas.

Tampoco puede denunciarse por este sistema ningún hecho en el que sus autores estén identificados.

- En comisaría: Acudiendo a alguna comisaría.

Enlaces de interés:

- Cuerpo Nacional de Policía: www.policia.es
- Guardia Civil: www.guardiacivil.org

ANEXO. NORMATIVA SOBRE SEGURIDAD PRIVADA

ANEXO. NORMATIVA SOBRE SEGURIDAD PRIVADA

- Ley 23/1992, de 30 de julio, de Seguridad Privada. Jefatura del Estado.

BOE Nº 186 de 4/8/1992

- Real decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada. Ministerio de Justicia e Interior.

BOE Nº 8 de 10/01/1995

Se dicta de conformidad con la Ley 23/1992, aprobándose reglamento de desarrollo.

- REAL DECRETO-LEY 2/1999, de 29 de enero, por el que se modifica la Ley 23/1992, de 30 de julio, de Seguridad Privada.

BOE Nº 26 de 30/01/1999

Modifica los arts. 7.1.b), 8.a) y 10.3.a) de la Ley 23/1992.

- Ley 14/2000, de 29 de diciembre, de Medidas fiscales, administrativas y del orden social. Jefatura del Estado:

BOE Nº 313 de 30/12/2000

Añade una disposición adicional quinta a la Ley 23/1992.

- REAL DECRETO-LEY 8/2007, de 14 de septiembre, por el que se modifican determinados artículos de la Ley 23/1992, de 30 de julio, de Seguridad Privada. Jefatura del Estado.

BOE Nº 225 de 19/09/2007

Modifica los arts. 1, 7, 9 y 10 de la Ley 23/1992.



CEA Confederación de
Empresarios de Andalucía



JUNTA DE ANDALUCÍA
CONSEJERÍA DE TURISMO, COMERCIO Y DEPORTE

CONFEDERACIÓN DE EMPRESARIOS DE ANDALUCÍA
C/ Arquímedes, 2. Isla de la Cartuja
41092 Sevilla
Tel.: 954 48 89 00
Fax: 954 48 89 11

<http://comercio.cea.es>

