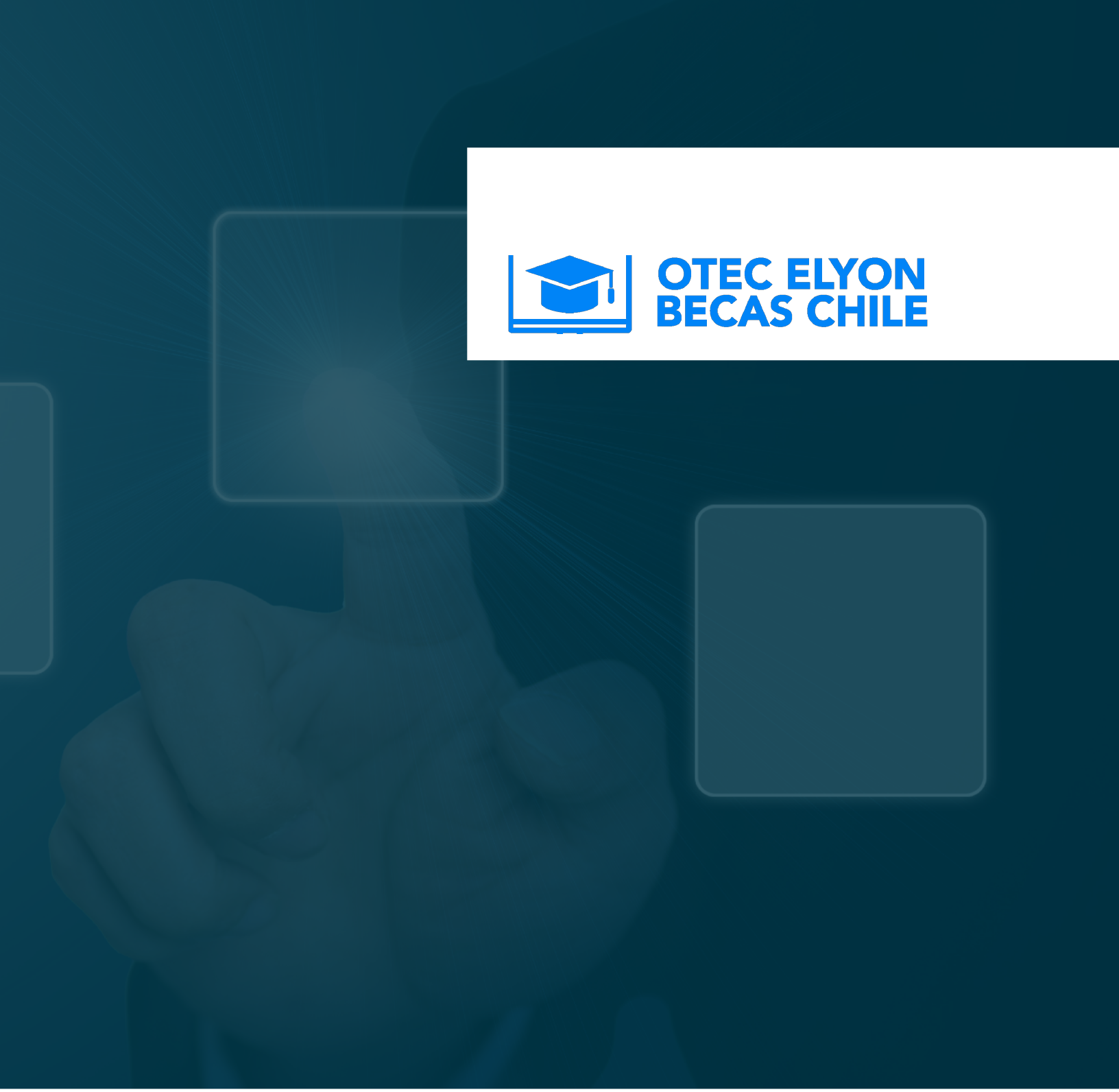


OTEC ELYON
BECAS CHILE

ENCARGADO DE SEGURIDAD
SEGURIDAD ELECTRÓNICA

07

MÓDULO
SEGURIDAD ELECTRÓNICA

Bienvenidos

I. Introducción

Hace 20 años hablar de seguridad representaba implicaciones como una persona encargada de realizar las labores de vigilancia, así como permitir o restringir el paso a personal autorizado o no autorizado, respectivamente. Seguridad en aquel entonces, también podía ser sinónimo de tener que recorrer instalaciones enteras para garantizar que todo estuviera en orden, o incluso se solía asociar el nivel de seguridad a los muros o rejas que definían el perímetro. En la actualidad, pueden mantenerse de alguna forma todas estas prácticas, pero de forma automatizada, mediante la utilización de la tecnología y las redes.

Con el paso de los años, los agigantados pasos que ha venido dando la tecnología, han logrado que las cosas que usualmente solían necesitar gran desgaste del personal humano o maquinaria rudimentaria para su funcionamiento, se reduzcan simplemente a equipos, desde los más complejos sistemas hasta los equipos más simples y pequeños, capaces de realizar grandes labores.

La seguridad electrónica se ha convertido en la bandera de los sistemas de seguridad en empresas, e incluso en hogares, y es hoy por hoy, el patrón fundamental de lo que a seguridad se refiere. Hablar de seguridad electrónica permite además pensar en la integración de múltiples sistemas y tecnologías, cuyo objetivo es el mismo: garantizar la integridad de los bienes y personas en las zonas a proteger. Sin embargo, es necesario conocer las necesidades de cada caso y las prestaciones que cada sistema puede ofrecer.

Los sistemas de circuito cerrado de televisión tienen años de penetración en el mercado, sin embargo ha sido recientemente que han venido cobrando mayor importancia por las prestaciones que brindan a los usuarios, la facilidad de

transmisión a través de redes LAN o de área local, y la facilidad de integración con otros sistemas de seguridad, así como su fácil administración. Actualmente, pensar en un sistema de CCTV implica pensar únicamente en la interconexión de cámaras a través de las redes, que no solo pueden ser locales, sino incluso a través de la más grande de todas las redes: Internet. La evolución de este sistema, le ha permitido no solo poder brindar conectividad IP, que facilita su instalación y administración, sino también la simplicidad de necesitar únicamente una cámara y un cable, a través del cual podemos no solo transmitir el video, sino también la alimentación eléctrica gracias a la tecnología conocida como PoE o Power Over Ethernet.

Por otra parte, los sistemas de Control de Acceso brindan facilidad y automatización en los procedimientos de ingreso y salida de determinadas áreas. Se basan únicamente en la verificación de información que se encuentra en bases de datos, las cuales pueden estar incluso a kilómetros de distancia, siempre y cuando se cuente con la conectividad necesaria a través de las redes.

La validación de la información puede realizarse con una tarjeta de proximidad, mediante características propias del individuo (como la huella dactilar, la voz o la pupila), con claves alfanuméricas, e incluso con combinaciones de las anteriores. Estas variaciones se conocen como 1:N, en donde se busca la coincidencia de la información suministrada entre N registros, o el método 1:1, en donde se valida la primera información para verificar que el registro exista, y una vez ubicado se procede a validar que la segunda información suministrada sea correcta.

Finalmente, como complemento, se suelen implementar sistemas de detección de intrusos, y es aquí donde tal vez exista más variedad y mayor flexibilidad para adaptarse a las necesidades de cada caso. Los sistemas de detección de intrusos, como su nombre lo indica, se basan en detectar patrones fuera de lo común en los perímetros definidos en la instalación de dichos sistemas, que pueden ser mediante rayos infrarrojo, rayos láser, cables sensores o señales microondas.

Adicionalmente, este tipo de sistemas puede ser de instalación superficial, aérea o subterránea, brindando así un sinfín de opciones para su uso.

Está tan claramente comprobado que la colocación de sistemas de seguridad electrónica disminuye considerablemente el riesgo de actos delictivos, que los Gobiernos no sólo a nivel nacional, sino internacional, están implementando sistemas de CCTV en las calles, avenidas y autopistas. Es por esta misma razón, que el conjunto de sistemas que conforman la seguridad electrónica, son básicos en el diseño de áreas de alta seguridad como bóvedas de bancos y centros de datos. Igualmente, gozan de gran popularidad en el ámbito laboral dentro de las grandes y medianas empresas.

2. Clasificación de los sistemas de seguridad electrónica

Definición:

Un sistema de seguridad puede ser definido como el conjunto de equipos y componentes necesarios para garantizar a las personas y bienes materiales, existentes en un determinado lugar, la protección necesaria frente a agresiones externas.

Los sistemas de seguridad pueden ser muy variables en función de las necesidades del usuario, de las características del recinto a proteger y del presupuesto disponible para ello. En el mercado existe un gran número de componentes con características técnicas muy distintas, que hacen que estos sistemas cuenten con una gran versatilidad.

Clasificación de los sistemas de seguridad.

Seguridad de las intalaciones		Seguridad Privada	
Sistemas de seguridad contra incendios.	Sistemas de detección de gas.	Sistemas antirrobo e intrusión	Circuito cerrado de televisión (CCTV)

Este tipo de sistemas pueden encontrarse ubicados en cualquier emplazamiento o edificación. La existencia de un sistema de seguridad electrónica en una instalación determinada puede ser obligatoria por ley en algunos casos (sucursales bancarias, hospitales, residencias, aeropuertos, garajes, cárceles, etc) o puede ser opcional, e instalarse simplemente por recomendación o por deseo expreso del propietario de la misma (vivienda particular, comercio, empresa, etc).

3. Sistemas de seguridad contra incendios

Tienen la finalidad de localizar un incendio lo más tempranamente posible y dar aviso del mismo, evitando que las llamas se propaguen y minimizando al máximo los daños que puedan producirse sobre las personas, bienes o inmuebles.

La respuesta ofrecida por este tipo de sistemas de seguridad ante la presencia de un incendio debe ser siempre la señalización acústica y luminosa, activando las correspondientes sirenas de alarma e indicadores que serán audibles y visibles en todo el perímetro del edificio. En caso de disponer de un sistema de extinción, entrará en funcionamiento automáticamente.

Dependiendo de la configuración previa y del tipo de instalación, el sistema puede también cortar los suministros de electricidad y gas o comunicar la situación de emergencia a un centro de alarmas que informará de la situación a los bomberos.

4. Sistemas de detección de gas

Los sistemas de detección electrónica de gas tienen como objetivo alertar a los usuarios de una instalación ante una o varias de las siguientes situaciones de riesgo:

- Riesgo de explosión por acumulación de gases o vapores inflamables.
- Riesgo de intoxicación por presencia de gases o vapores tóxicos.
- Riesgo de asfixia por falta de oxígeno.
- Riesgo de explosión por exceso de oxígeno.

Estas atmósferas tóxicas, inflamables o explosivas pueden haber sido generadas por diferentes tipos de gases, como por ejemplo propano, metano, butano, gas natural, monóxido de carbono, oxígeno, hidrógeno, dióxido de carbono, propileno, etc.

En consecuencia, los principios de medición y los criterios de instalación y montaje de los dispositivos del sistema dependerán del tipo de vapor o gas a detectar en cada caso.

5. Sistemas antirrobo e intrusión

Se designa genéricamente como sistema de seguridad electrónica anti-intrusión al conjunto de equipos y elementos capaces de gestionar una o varias de la siguientes funciones:

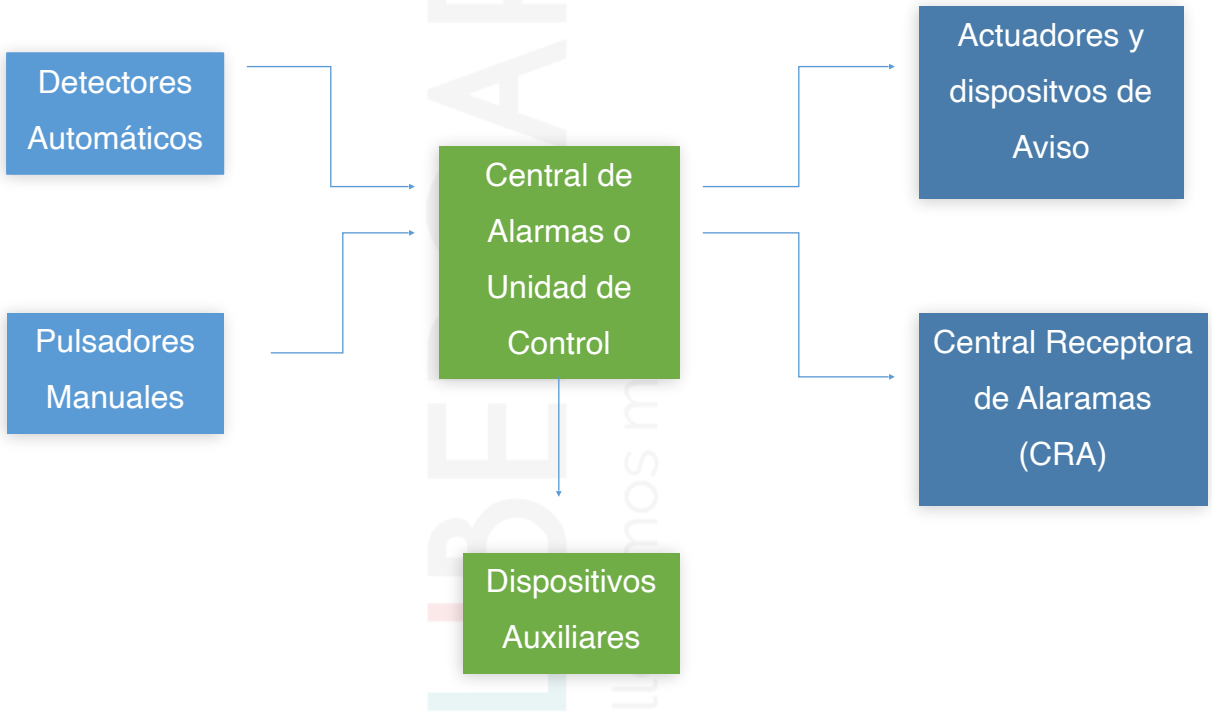
- **Intrusión.** Los dispositivos anti-intrusión advierten cualquier intento de irrupción o allanamiento en un determinado perímetro o recinto.
- **Robo o atraco.** Los dispositivos antirrobo o anti atraco previenen los ataques contra personas, bienes e inmuebles.
- **Control de presencia.** Los dispositivos de control de presencia detectan el movimiento o existencia de personas en determinadas zonas de una edificación.
- **Control de accesos.** Los dispositivos de control de accesos permiten registrar y gestionar la entrada y salida de personas y vehículos a un determinado recinto o zona.

6. Circuito cerrado de televisión (CCTV)

Un circuito cerrado de televisión, más conocido por su acrónimo CCTV, es aquel que permite visualizar y en algunos casos grabar imágenes captadas por una serie de cámaras para controlar en tiempo real determinadas zonas de una instalación.
Estos sistemas basan su funcionamiento en una serie de cámaras, monitores y otros dispositivos de tratamiento de la señal de audio y video, pudiendo incluso enviar imágenes de manera remota a través de Internet.

7. Elementos que constituyen un sistema de seguridad

Bloques funcionales que componen un sistema electrónico de seguridad



8. Central de alarmas.

La central de alarmas, también conocida como unidad de control o unidad de proceso, es el elemento fundamental del sistema. Se encarga de recibir información en forma de señales procedente de los sensores, interpretarla en función de la programación preestablecida y enviar la información correspondiente hacia los actuadores para que ejecuten las órdenes correspondientes.

La central de alarmas proporciona la alimentación a todos los componentes de la instalación conectados y, en algunos casos, es capaz de transmitir la señal de alarma a destinos externos, como a un local de vigilancia, a la policía o a los

bomberos, al dispositivo móvil del propietario de la instalación, etc. Puesto que se encarga de gestionar todo el sistema, esta unidad de control es considerada el **cerebro del sistema** de detección electrónica.

La mayoría de las centrales de alarmas se encuentran ubicadas en una envolvente metálica o de plástico de fijación mural. Internamente están formadas por los componentes necesarios para analizar y gestionar la información y para suministrar la tensión de funcionamiento a todos los dispositivos conectados a la misma. Estos componentes se dividen en 6 grupos:

Placa Base.

Se trata de una tarjeta de circuito impreso a la que se encuentran conectados los componentes electrónicos que forman parte de la central. Se encuentra localizada en el interior de una envolvente de plástico o metal y dispone de una serie de conectores y zócalos para instalar o centrar componentes.

Microprocesador.

Es el componente electrónico que recibe y procesa toda la información proveniente de los sensores y envía las órdenes correspondientes hacia los actuadores, por lo que se trata del verdadero cerebro de la instalación. Dependiendo de las características y el nivel tecnológico del microprocesador, la central permitirá un mayor o menor número de posibilidades de configuración y gestión.

Memorias.

Son componentes electrónicos integrados en la placa base en los que se almacenan las instrucciones y la configuración del sistema de detección.

Teclado o panel de control.

Situado en la parte frontal de la unidad de control, está compuesto por un display, teclas alfanuméricas e indicadores luminosos. Se utiliza para apagar y encender la instalación de alarma, programar las funciones de la central y verificar el estado del sistema.

Fuente de alimentación.

Suministra la tensión constante necesaria para el funcionamiento de la central de alarmas. Incorpora un transformador y un rectificador que convierte la tensión de la red eléctrica (230 V) en al tensión de funcionamiento del sistema (generalmente 12 a 24V).
En las instalaciones donde el número de dispositivos existentes es muy elevado resulta necesario utilizar fuentes de alimentación secundarias, que suelen estar distribuidas por plantas.

Baterías.

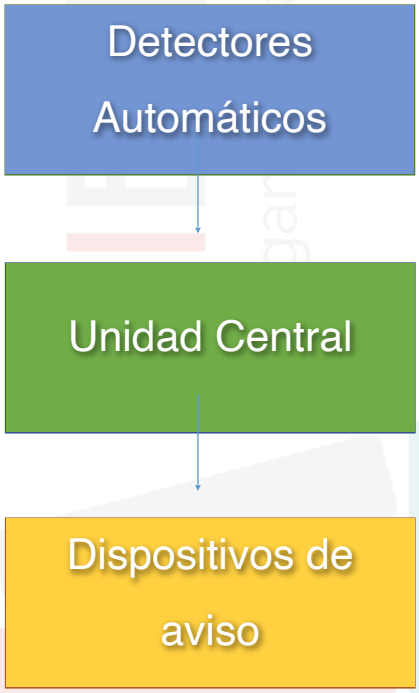
Como medida de seguridad, las baterías se colocan en el interior de la envolvente de la central para prevenir cualquier posible fallo en el suministro eléctrico ordinario. El uso de estas baterías secundarias asegura el funcionamiento del sistema durante un periodo de tiempo determinado.

El nivel de tensión ofrecido por al baterías utilizadas en este tipo de instalaciones suele ser normalmente de 12 V, con unas intensidades que oscilan entre 2,2 y 26 Ah.

9. Detectores automáticos y pulsadores manuales

Los detectores automáticos o sensores, junto con los dispositivos de pulsación manual, componen lo que se denomina como entradas del sistema. Son dispositivos de tamaño reducido.

Las entradas se encargan de medir variables físicas externas o captar determinados eventos, como variaciones de presión, sonidos, etc., y envían la información correspondiente en forma de señales eléctricas hacia la central de alarmas.



10. Red de actuadores y dispositivos de aviso

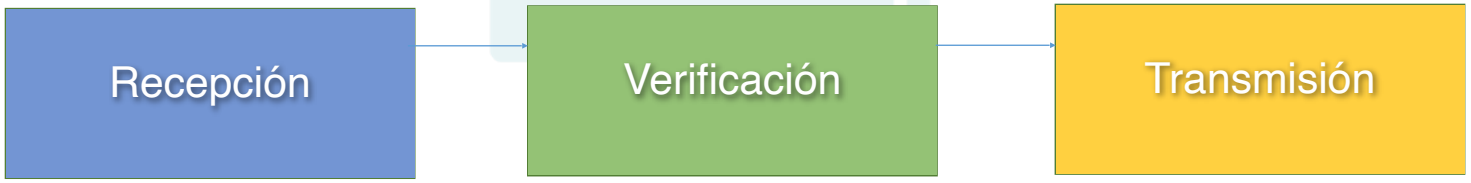
Los actuadores, o **salidas del sistema**, son los dispositivos encargados de recibir la información procedente de la central de alarmas y ejecutar las acciones para las que han sido diseñados.

Tienen la consideración de actuadores todos los dispositivos de aviso acústicos y ópticos (alarmas, serenas campanas o bocinas), los dispositivos de señalización (flashes y señales indicadoras luminosas), las alarmas silenciosas, el alumbrado de emergencia, los sistemas de extinción de incendio, las cerraduras electrónicas, los retenedores electromagnéticos de puertas cortafuegos, etc.

11. Central receptora de alarmas (CRA)

La Central Receptora de Alarmas (CRA) ofrece un servicio de recepción, verificación y gestión de alarmas a distancia. Es propiedad de una empresa de seguridad homóloga y autorizada por el ministerio de Industria y está controlada por el personal debidamente especializado.

Debe estar disponible 24 horas todos los días del año y puede ofrecer también otras funciones tales como video vigilancia continuada, gestión y control remoto de instalaciones, registro de eventos, envío de informes de estado, etc.



Tras recibir la alerta provocada por un sistema de seguridad, los operadores de la Central Receptora de Alarmas analizan la información, y en caso de verificarse el estado de alarma se ofrece una respuesta de actuación atendiendo a las instrucciones de operativa establecidas previamente por cada cliente:

- Transmisión de la alarma a las Fuerzas y Cuerpos de seguridad del Estado.
- Transmisión de la alarma a los Bomberos y otros servicios de Urgencia.
- Comunicación directa con el propietario de la Instalación.

Las centrales Receptoras pueden ofrecer sus servicios simultáneamente a miles de instalaciones a nivel nacional e internacional, utilizando siempre conexiones seguras (GSM, TCP/IP, GPRS, etc) que permiten procesar y almacenar todos los avisos recibidos.

Un sistema de seguridad sólo puede ser conectado a una CRA o aun centro de control cuando la instalación haya sido realizada por una empresa de seguridad autorizada para dicha actividad.

12. Dispositivos auxiliares

Los equipos y dispositivos auxiliares pueden ser utilizados para mejorar las características funcionales o aumentar las prestaciones de un sistema de seguridad electrónica. Entre otras funciones, optimizan las tareas de gestión, control y detección y facilitan las comunicaciones internas y externas de la instalación.

Los dispositivos auxiliares más utilizados actualmente son los paneles repetidores, las interfaces de comunicación (RS-232, radio, GSM, Bluetooth, etc), los teclados, los módulos comunicadores, los módulos de ampliación, los expansores de zonas, los paneles de control, etc.

13. Medios de comunicación entre componentes

Los equipos y componentes que forman parte de una instalación de seguridad electrónica envían o reciben la información utilizando señales eléctricas o electromagnéticas.
Atendiendo al medio de comunicación o transmisión a través del cual se transportan dichas señales, estos sistemas pueden clasificarse en cableados e inalámbricos.

14. Sistemas cableados

Los componentes de un sistema cableado se comunican con la central de alarmas mediante líneas de comunicación específicas, como pueden ser el cable convencional, cable bus, cables pares, cable coaxial, fibra óptica, etc.

Este tipo de sistemas presentan como principal ventaja su fiabilidad y robustez, puesto que las señales que contienen la información prácticamente no están expuestas a interferencias externas.

Sin embrago, la instalación del cableado y las correspondientes canalizaciones hacen que el montaje sea más sofisticado y costoso. Las distancias a las que pueden estar conectados los quipos con respecto a la central dependen de las características del cable utilizado en cada caso.

15. Sistemas inalámbricos

Los componentes de un sistema inalámbrico se comunican con el panel de alarmas a través de señales infrarrojas o de radio frecuencia encriptados, utilizando el aire como medio físico para el transporte de la información.

La ventaja de este tipo de sistemas radica en que no precisan ningún tipo de cableado ni canalización y pueden abarcar un radio de acción muy amplio, por lo que ofrecen gran flexibilidad en la instalación de los componentes y el montaje se realiza de manera sencilla y en muy poco tiempo.

Los inconvenientes asociados a utilizar un sistema inalámbrico son 2: necesitan mucho mantenimiento (puesto que todos los quipos funcionan mediante pilas o baterías que es necesario revisar y sustituir periódicamente) y son susceptibles a interferencias externas producidas por emisiones de radio frecuencia o electromagnéticas (teléfonos móviles, radio, televisión, etc), lo que les hace más vulnerables ante posibles sabotajes.

16. Sistemas de comunicación remota.

Existen tecnologías de comunicación cableada e inalámbrica que se utilizan para transmitir la información hacia el exterior del sistema, como por ejemplo, al dispositivo móvil del propietario de la instalación o una CRA. En la actualidad, los sistemas de comunicación remota más utilizados en detección electrónica son los siguientes:

- Transmisión vía satélite
- Transmisión por telefonía fija
- Transmisión por telefonía móvil (GSM, GPRS, etc)
- Transmisión vía radio
- Transmisión por tecnología Wi-Fi
- Transmisión por tecnología Bluetooth
- Transmisión a través de una red de datos local (LAN)
- Transmisión a través de Internet (TCP/IP)

17. Falsas Alarmas.

Independiente del grado de fiabilidad y seguridad que proporciona un sistema de seguridad electrónica, pueden producirse situaciones inesperadas que desencadenan la activación de los dispositivos de alarma sin motivo aparente. Estas situaciones anómalas, son denominadas **falsas alarmas.**

Las falsas alarmas pueden ser desencadenadas por factores muy diversos como:

- Una inadecuada instalación inicial.
- Fallos de funcionamiento de los detectores o en la central.
- Ajustes incorrectos en los detectores.
- Baja calidad de los equipos.
- Deterioro de los componentes.
- Factores ambientales (iluminación, temperatura, lluvia, nieve, etc)
- Modificaciones en el entorno.
- Presencia de mascotas o animales.
- Intrusos que son disuadidos por al activación de las sirenas.
- Subidas de tensión eléctrica.

En cualquier tipo de sistema de seguridad, un menor número de falsas alarmas proporciona mayor grado de fiabilidad y seguridad, que es en definitiva el objetivo de la instalación. El principal inconveniente asociado a un alto valor en el índice de falsas alarmas, es que el usuario acaba por dejar de hacer caso al sistema, facilitando que se produzcan situaciones de riesgo potencial. El objetivo de todo sistema de seguridad es, por tanto, ser inmune a las falsas alarmas. Esto se consigue a través de un correcto proceso de diseño, instalación, puesta en marcha y mantenimiento de todos los componentes del sistema. Cabe destacar, que la transmisión de una alarma no confirmada a las Fuerzas y Cuerpos de Seguridad, que resulten falsas, podrá ser objeto de denuncia para la imposición de la correspondiente sanción.

Sistema de Alarmas

1. Control de Accesos

Los sistemas de control de acceso son la tecnología con más demanda en el mercado actual, hemos migrado de sistemas mecánicos y con personal especializado, a tener procesos de control de entrada y salida completamente automatizados con diferentes tipos de tecnologías y dispositivos. Es importante realizar un estudio adecuado, segmentando las zonas, los grupos de acceso, los horarios permitidos, el nivel de acceso de cada usuario, medir la cantidad de personas o carros que transitan por cada zona y establecer claramente los objetivos de cada control de acceso.

Es importante el estudio y diseño previo a cualquier instalación y puesta en marcha de un proyecto de seguridad y control de acceso. Una adecuada integración de los dispositivos electrónicos con los dispositivos electromecánicos permitirá incluso reducir drásticamente los costos de personal y totales del proyecto, haciendo incluso que un sistema de control de accesos se pueda pagar literalmente solo en un tiempo muy corto.

Beneficios

- Control de Entradas y Salidas
- Mayor Seguridad y Control del Público
- Ahorro en Costos de Personal
- Disminución en Tiempo de Registro
- Mejoramiento en la Productividad del Personal
- Permitir/Restringir la Apertura de Puertas
- Valorización Monetaria de la Edificación
- Valor Agregado en Modernización

2. Control de acceso peatonal

Los sistemas de control de accesos peatonales se implementan para tener el control de todo el personal que transita en un espacio público o privado, asegurando el paso de personas que cuentan con un libre tránsito y restringiendo el paso de personas no autorizadas en áreas específicas. Las soluciones para control de accesos peatonales son muy variadas dependiendo de las aplicaciones y las necesidades de cada cliente, se pueden tener desde soluciones con un solo dispositivo que controla una puerta, hasta soluciones con múltiples dispositivos integrados a diferentes sistemas electromecánicos gestionados por medio de software centralizado.

Beneficios y ventajas

Al implementar una solución para control de accesos peatonales podemos:

- Incrementar la seguridad del edificio, teniendo la certeza que únicamente ingresan personas autorizadas.
- Ahorrar en los costos y gastos fijos en personal.
- Agilidad en los tiempos de entrada y salida ya que el personal autorizado esta previamente registrado en las bases de datos y no se tiene que hacer un registro completo diario.
- Mayor control y gestión de todo el personal, trabajadores y visitantes.
- Integración con todos los sistemas de seguridad para lograr una gestión más eficiente de todo el edificio.

3. Lector De Huellas Digitales

Este es una forma de control biométrico utilizada muy a menudo como parte integral de un sistema de control de acceso. Los sistemas biométricos forman parte de una gran gama de alternativa usadas para la identificación de individuos. Esto se debe a que los sistemas biométricos hacen un análisis de cualidades personales únicos en cada individuo, como lo son las huellas dactilares, la retina, el iris y la geometría de la mano. El lector de huellas dactilares es la forma de control biométrico más popular y más eficiente en la verificación e identificación para control de accesos.

Ventajas	Aplicaciones
Identificación rápida en el dispositivo (menos de 1seg)	Edificios de oficinas
Identificación única por cada usuario	Edificios comerciales
No es necesario memorizar claves	Conjuntos y edificios residenciales
No es necesario cargar con tarjetas o controles	
La huella dactilar no es posible extraviarla	
No genera costo extra para cada usuario	
Integración con toda una gama de productos	

4. Tarjeta de proximidad

Las tarjetas de control o proximidad son de gran aplicación en los sistemas de control de acceso, ya que estas nos permiten tener toda la información de cada usuario y además es posible personalizarlas con la imagen corporativa de la empresa y cualquier información impresa necesaria sobre la tarjeta. Tienen una gran aplicación en el control de asistencia y visitante. La mayor ventaja radica en la capacidad de darle autorización a puertas o zonas específicas dentro de la edificación, generando seguridad y control sobre el acceso de las personas.

Ventajas	Aplicaciones
Toda la transmisión de datos por radio frecuencia entre la tarjeta y el lector es encriptada utilizando un algoritmo de seguridad.	Edificios de oficinas
Se reduce el riesgo de poner en peligro la seguridad de la información o copiar las tarjetas sin autorización.	Edificios comerciales
Se visualiza como un carnet dentro del edificio o empresa.	Conjuntos y edificios residenciales
Costo de reemplazo bajo.	Conjuntos y edificios Hoteles
Personalización de cada tarjeta tipo carnet. En caso de pérdida solo se desactivan en el software.	Conjuntos y edificios Hospitales

5. Combinación en Controles de Accesos

Según la aplicación es posible combinar diferentes tipos de autenticación en un solo dispositivo. De este modo, podemos aumentar la seguridad de nuestras instalaciones. Como Encargado de Seguridad, es posible realizar revisiones de las áreas de la empresa que podrían ser vulnerables, por lo que es fundamental familiarizarse con la mayor cantidad de sistemas posibles. A modo de ejemplo y con fines de ejemplificación, podemos realizar las siguientes combinaciones:

Combinaciones	Aplicaciones
Huella dactilar + clave	Entradas principales
Tarjeta de proximidad + clave	Bodegas
Huella dactilar + tarjeta de proximidad	Bancos
Huella dactilar + tarjeta de proximidad + clave	Depósitos
	Joyerías y Comercio

6. Torniquetes de acero

El Torniquete está indicado para control de los accesos peatonal en zonas de alto tránsito de personas. Es ideal como barrera de control para sitios donde se desee regular el flujo de personas en las operaciones de entrada y salida. Es perfectamente compatible e integrable con todos los otros dispositivos de control de accesos según sea la aplicación. Los torniquetes de acceso son mecanismos electromecánicos de alta confiabilidad, construidos con la más alta tecnología teniendo en cuenta que serán sometidos a las más duras condiciones de uso y desgaste. La robustez de todos sus componentes asegura un funcionamiento libre de fallas con un mínimo mantenimiento realizado por nuestros técnicos. En su fabricación y diseño se tiene en cuenta las condiciones ergonómicas y elementos hidráulicos que facilitan el uso para personas de edad avanzada, mujeres en embarazo, niños y personas con discapacidad.

Aplicaciones
Edificios con alto flujo de personas
Estadios
Áreas deportivas
Acceso a Centros recreativos
Estaciones ferroviarias, marítimas y subterráneas

7. Puertas de seguridad

Las puertas de seguridad, o puertas corredizas, funcionan mediante diferentes sistemas electromecánicos: Sliders, electroimanes, cantoneras eléctricas, sensores y brazos para puertas batientes. En general es posible automatizar la mayoría de puertas de control de accesos para obtener una mayor seguridad y ahorro. También son completamente integrables a los dispositivos de control de acceso, para obtener un sistema completo.

Ventajas	Aplicaciones
Ajuste de la velocidad de apertura	Centros comerciales
Diseñadas para funcionamiento continuo	Supermercados
Apertura sin necesidad de tocar las puertas	Edificios de oficinas
Detección de presencia y movimiento	Fachadas para conjuntos y edificios residenciales
Soluciones para variedad de ambientes y dimensiones	
Total cumplimiento con todos los estándares y normatividad de la construcción	

8. Video Portero

El video portero es una excelente solución cuando se quiere realizar una verificación antes de dar permiso de acceso al visitante. Se realiza la verificación de la persona, se establece la comunicación y una vez la persona es autorizada se realiza la apertura de la puerta remotamente.

Ventajas	Aplicaciones
Video y audio para tener una mayor seguridad	Edificios residenciales
Placa exterior con tele cámara, auto iluminación para visión nocturna y síntesis de voz	Edificios de oficinas
Integración con el abre puertas eléctrico	Oficinas y Bodegas

9. Tarjetas con banda magnética.

Una banda magnética (llamada a veces *magstripe* como abreviación de *magnetic stripe*) es toda aquella banda oscura presente en tarjetas de crédito, abonos de transporte público o carnés personales que está compuesta por partículas ferromagnéticas incrustadas en una matriz de resina (generalmente epoxi) y que almacenan cierta cantidad de información mediante una codificación determinada que polariza dichas partículas. La banda magnética es grabada o leída mediante contacto físico pasándola a través de una cabeza lectora/escritora gracias al fenómeno de la inducción magnética. En aplicaciones estándar de tarjetas de identificación, como las usadas para las transacciones financieras, la información contenida en la banda magnética se organiza en diferentes pistas. Estas tarjetas contrastan con la nueva generación de tarjetas inteligentes que contienen un chip con contactos metálicos, o tarjetas sin contacto que usan un campo magnético o radiofrecuencia (RFID) para la lectura a una distancia media.

Ventajas	Aplicaciones
Se visualiza como un carnet dentro del edificio o empresa	Edificios de oficinas, Hoteles y edificios comerciales
Costo de reemplazo bajo	Conjuntos y edificios residenciales
Personalización de cada tarjeta tipo carnet	Conjuntos y edificios Empresas
En caso de pérdida solo se desactivan en el software	Conjuntos y edificios Hospitales
Integración con toda una gama de productos electromecánicos y puertas automáticas.	

10. RECONOCIMIENTO DE VOZ

El reconocimiento por voz o parlante, es una modalidad biométrica que utiliza la voz de un individuo con fines de reconocimiento. (Difiere de la tecnología del "reconocimiento de discurso", que reconoce las palabras a medida que van siendo articuladas, este no es un dispositivo biométrico). El proceso de reconocimiento de voz depende de las características de la estructura física del tracto vocal de un individuo así como también de sus características de comportamiento.

El reconocimiento por voz es una elección popular de reconocimiento biométrico remoto, dada la disponibilidad de dispositivos para tomar las muestras de voz (por ejemplo: la red telefónica y los micrófonos de las computadoras) y su facilidad de integración. El reconocimiento del orador, es una tecnología biométrica distinta de otras en las que la muestra de discurso es tomada dinámicamente o en el lapso de un periodo de tiempo determinado, como pueden ser algunos segundos. El análisis ocurre en un modelo en el que los cambios a lo largo del tiempo son monitoreados, lo que es similar a otros dispositivos biométricos que contemplan el comportamiento, como pueden ser: la firma dinámica, el reconocimiento de la forma de andar, y el reconocimiento por el ritmo de las pulsaciones en un teclado.

Ventajas	Aplicaciones
Identificación única por cada usuario	Edificios de oficinas
No es necesario memorizar claves	Edificios comerciales
No es necesario cargar con tarjetas o controles	Conjuntos y edificios residenciales
La voz no es posible extraviarla	
No genera costo extra para cada usuario	
Integración con toda una gama de productos electromecánicos y puertas automáticas	

11. Reconocimiento de Iris y Retina

La utilización del ojo humano en la identificación de personas ha dado lugar a dos técnicas biométricas diferentes: una basada en las características del iris ocular y otra que utiliza las características distintivas de la retina. Únicamente tienen en común que se sirven de un mismo órgano, el ojo humano, sin embargo en numerosas ocasiones se suele confundir uno con otro y ambas se consideran como una única técnica denominada biometría del ojo, por lo tanto es importante resaltar que el iris y la retina oculares dan lugar a dos tipos de sistemas biométricos completamente diferentes, tanto en los métodos de captura de imagen y las técnicas de extracción de características como en los métodos de comparación.

Ventajas	Aplicaciones
Identificación única por cada usuario	Edificios de oficinas
No es necesario memorizar claves	Edificios comerciales
No es necesario cargar con tarjetas o controles	Conjuntos y edificios residenciales
La retina e iris son únicas para cada usuario	
No genera costo extra para cada usuario	
Integración con toda una gama de productos electromecánicos y puertas automáticas	

12. Control de Acceso Vehicular

Los sistemas de control de accesos vehicular se implementan para tener el control de los vehículos que circulan por un espacio público o privado, asegurando el paso a los vehículos permitidos y restringiendo a aquellos que no estén autorizados. Al integrar un sistema de control de accesos vehicular, podemos tener el control total, tanto de los residentes como de los visitantes.

Se integran sistemas biométricos de identificación, sistemas de visión artificial para reconocimiento de placas, sistemas de identificación por radio frecuencia para activar las puertas sin necesidad de abandonar los vehículos, y la total integración con otros software de gestión, que en conjunto aseguran las mejores soluciones para cada proyecto.

Ventajas

- Ahorro en personal extra dedicado a la vigilancia y control de acceso vehicular.
- Mayor seguridad con registros de entradas y salidas, horarios, grupos de acceso, zonas permitidas
- Base de datos con toda la información necesaria: placas, descripción del vehículo, propietario, datos de contacto y toda la información que se considere necesaria para un correcto control de acceso vehicular.
- Ingreso de automóviles de forma controlada y organizada.
- Sistema automatizado mejorando el acceso vehicular.
- Reconocimiento de placas para aplicaciones de avanzadas.
- Asociación de las placas con la identificación del conductor para mayor seguridad.
- Reconocimiento de TAGs RFID para aplicaciones manos libres.
- Alertas en caso de un intento de acceso sin autorización.
- Integración con todos los sistemas de seguridad para una gestión centralizada.
- Conexión e integración con la red IP para monitoreo desde diferentes puntos.

13. Control Biométrico Vehicular

En nuestro sistema de control de acceso vehicular es posible utilizar lectores biométricos, tarjetas de control, claves y combinaciones. Estos sistemas biométricos pueden ser instalados estratégicamente teniendo en cuenta el fácil posicionamiento de cada vehículo y el diseño de la instalación. En efecto, realizamos el diseño del pedestal personalizado para cada instalación teniendo en cuenta factores de accesibilidad, exposición a la lluvia y al sol, protección del mismo dispositivo y facilidad en la autenticación de cada usuario. Cada sistema biométrico se comunica con el software de gestión para tener un control de accesos vehicular completo con toda la funcionalidad.

Ventajas	Aplicaciones
Activación de puertas y barreras automáticamente	Centros comerciales
Activación de puertas y barreras automáticamente	Parking
Integración con tickets o huellas dactilares	Edificios comerciales
Notificación de placas no autorizadas	Edificios y conjuntos residenciales
Notificación intento de hurto	Edificios de oficinas
Integración con todos los sistemas de seguridad	
Consulta y registro en base de datos	

14. Reconocimiento de Placas

El sistema de reconocimiento de placas es una solución de avanzada para un control de accesos vehicular donde las exigencias de seguridad sean máximas. El reconocimiento de matriculas se hace de forma automática sin necesidad de un operario. Nuestro sistema tiene en cuenta los diferentes niveles de luminosidad que se puedan presentar a diferentes horas del día, los diferentes posicionamientos de los carros, condiciones de intemperie, deterioro de las placas, diferentes alturas y en general todas las variables que puede presentar el sistema. Las cámaras de alta resolución con visión artificial se complementan al software de gestión y a los sistemas electromecánicos para poder realizar un acceso vehicular seguro, personalizado y de acuerdo a las necesidades específicas del proyecto. Es posible asociar el sistema a un generador de tickets o un lector de huella dactilar del conductor para una mayor seguridad.

Ventajas	Aplicaciones
El vehículo no se tiene que detener	Peajes
Agiliza el transito	Entradas vehiculares plantas industriales
Evita el manejo de dinero en efectivo en las casetas	Estacionamientos de buses y sistemas de transporte masivo
TAG con código de identificación único	Entradas y salidas obras civiles
El TAG no necesita batería	
Rápida velocidad de lectura	
Interoperabilidad con otras zonas	
Integración con sistemas electromecánicos, por lo general se utilizan las barreras	
ntegración con los semáforos de señalización	

15. Acceso Vehicular RFID Identificación por Radio Frecuencia

La solución RFID realiza una identificación del vehículo por radio frecuencia, esto quiere decir que no hay necesidad de bajarse del carro o sacar la mano por la ventana para autenticarse o entregar dinero a una operadora. Una antena ubicada estratégicamente lee el TAG o Etiqueta que se encuentra en el vehículo. El sistema de control de accesos vehicular basado en RFID permite un acceso vehicular al mismo tiempo que acciona los sistemas electromecánicos, de esta forma el conductor no tiene que detenerse. Es un sistema muy eficiente para lugares en los cuales no es necesaria la identificación del conductor y la asociación del mismo con el carro. Sin embargo, si es posible identificar el carro y para soluciones en peajes se puede saber el saldo con el que cuenta el TAG para permitir el paso automático o negarlo.

Ventajas	Aplicaciones
Autenticación con huella dactilar, tarjetas de proximidad y/o clave	Entradas vehiculares a conjuntos residenciales
Integración con todos los sistemas de seguridad del edificio	Entradas vehiculares a edificios residenciales
Fácil e intuitivo manejo por parte de los usuarios	Entradas vehiculares a edificios de oficinas
Software intuitivo para administración del sistema	
Pedestales personalizados para cada solución	
Integración con los dispositivos electromecánicos	
Permite crecimientos futuros	

16. Barreras Vehiculares Automáticas

Las barreras de estacionamiento las utilizamos en integración con los controles de accesos vehicular para un correcto manejo del flujo vehicular en un determinado parqueadero. Su principal función se basa en permitir e impedir el paso a los vehículos, realizando la tarea de forma automática, eficiente, rápida y segura. Las barreras vehiculares cuentan con sistemas de anti-aplastamiento que impiden que un vehículo sea golpeado en caso de no avanzar rápidamente en la zona de accionamiento. Se cuentan con barreras de estacionamiento automáticas para distintas aplicaciones: barreras sencillas, barreras con bastidor articulado, barreras con cerca de protección, barreras de corto y largo alcance.

Ventajas	Aplicaciones
Accionamiento e integración con todos los dispositivos de control de accesos	Centros comerciales
Trabajo continuo	Edificios de oficinas y consultorios
Sistema anti-aplastamiento y destrabe manual	Parking
Tiempo de apertura rápido de 2 a 4 segundos dependiendo del modelo	Peajes
	Entradas vehiculares plantas industriales
	Estacionamientos de buses y sistemas de transporte masivo
	Entradas y salidas obras civiles

17. Sistemas de Alarmas

Un sistema de alarma es una barrera de tipo electrónica, su función principal es comunicar a través de un dispositivo de sonido o luz la penetración de un intruso a la instalación, al mismo tiempo. Este dispositivo ahuyentará al intruso. Un sistema de alarma se compone de las siguientes señales de alarma: Señal de robo, Señal de asalto, Señal de pánico y Señal de incendio.

18. Señal de Robo

Se utilizan cuando la instalación se encuentra sin personal en su interior protege las puertas, ventanas, los muros, techos, entre otros. También puede utilizarse como protección perimetral. Al activarse produce un sonido. Funciona sólo cuando la instalación se encuentra cerrada. Elementos técnicos usados:

- Rayos infrarrojos pasivos (zona interior)
- Sensores fotoeléctricos (zona exterior)
- Magnéticos (puertas y ventanas)
- Detectores de vibración (muros, techos, tabiques)
- Detectores de quiebre (vidrios vitrinas)
- Discriminadores de audio (vitrinas, ventanales, mamparas)

Rayos Infrarrojos Pasivos: Un sensor infrarrojo pasivo (o sensor PIR) es un sensor electrónico que mide la luz infrarroja (IR) radiada de los objetos situados en su campo de visión. Se utilizan principalmente en los detectores de movimiento basados en PIR.

Sensores Fotoeléctricos: Un sensor fotoeléctrico o fotocélula es un dispositivo electrónico que responde al cambio en la intensidad de la luz. Estos sensores requieren de un componente emisor que genera la luz, y un componente receptor que percibe la luz generada por el emisor.

Sensores Magnéticos: El contacto magnético se utiliza para la protección de puertas y ventanas, en cuanto se separa la hoja de la puerta o ventana unos centímetros se cierra o abre el circuito , según sea el modelo, y la central produce una alarma.

Detectores de Vibraciones: Dispositivo integrado por un elemento sensible a la rotura de cristales, de dimensiones pequeñas (3 a 5 cm de diámetro y de 2 a 7 cm de alto) que permite detectar desde el rayado mediante herramienta de corte hasta la rotura total del cristal según el modelo que se elija.

Detectores de Quiebre: “Detector de rotura de cristales con contacto de mercurio”; en este caso, dentro del detector existe un bulbo sellado al vacío que contiene dos delgadas varillas metálicas conductivas, cortocircuitadas por una pequeña gota de mercurio. Esta gota de mercurio salta de su asiento natural, en presencia de un impacto fuerte sobre la superficie acristalada, interrumpiendo el circuito y señalizando una alarma; lo mismo ocurrirá si el cristal se rompe y cae el pedazo de cristal arrastrando al detector consigo.

Discriminadores de audio: Los detectores de rotura de cristal-deben montarse en una pared o el techo y que puede cubrir un área de 35 pies, no importa en qué dirección. Ellos tienen algunas desventajas, porque no pueden oír a través de las paredes o en las esquinas.

Barrera Infrarojos: La barreras de infrarrojos se usan para la detección perimetral de intrusión se realiza, como su nombre indica, sobre el perímetro de la vivienda o parcela. Este equipo se conforma de dos partes separadas entre sí: un emisor que envía continuamente un haz infrarrojo invisible en forma pulsada y codificada y un receptor sensible a él. Al interrumpirse el haz de pulsos codificado, el receptor informa de tal evento a la central.

Barreras Microondas: El funcionamiento de las barreras de microondas es muy simple. Este tipo de dispositivos genera un haz electromagnético de microondas de alta frecuencia desde el transmisor hasta el receptor, creando un muro de protección invisible pero sensible. Cuando el receptor detecta una diferencia dentro del haz (y por lo tanto una posible intrusión) se inicia un análisis detallado de la situación que, si se considera una intrusión real, proporciona una señal de alarma que puede ser tratada de forma analógica o digital.

Cable Enterrado: Es un sensor enterrado de detección de intrusiones, para la seguridad de perímetros exteriores, que genera un campo de detección de radar invisible alrededor de los cables sensores enterrados. Si un intruso perturba el campo, se activa una alarma y se determina el lugar de la intrusión.

Superficie Pavimentada: Este sistema es perfecto para superficie pavimentada con base de cemento. Está especialmente diseñado para puntos de accesos como puertas o ventanas, así como paso de vehículos o peatonales. El sistema crea un área invisible capaz de detectar la presencia humana. Está preparado para varios tipos de pavimentos y puede operar en condiciones meteorológicas duras.

Video Sensor: El videosensor es un sistema de los llamados “inteligentes”, cuya función es la detección de movimiento mediante un análisis de vídeo. El sistema funciona con una serie de cámaras instaladas de manera estratégica para dar cobertura visual a la zona. Este sistema de seguridad es muy eficaz ya que está diseñado para ser capaz de detectar varios intrusos a la vez por cada escena tomada por la cámara, que supervisa una amplia zona.

Barreras Infrarrojos Para Ventanas: Se trata de barreras de infrarrojos diseñadas específicamente para ofrecer una máxima seguridad en puertas, ventanas y zonas de fácil escalada. Cuando los haces que proyectan son atravesados (significa que un intruso ha atravesado una puerta o ventana de su casa), entonces el sistema manda una señal a la central que se pondrá en contacto con los cuerpos de seguridad pertinentes. Con todo, usted tiene una amplia variedad en sistemas de alarma perimetral que le permitirán elegir el que mejor se adapte a sus necesidades.

19. Señal de Asalto

Sistema de alarmas utilizadas en instituciones que manejen bienes y valores en conjunto con atención de público como por ejemplo bancos, cajas, cajeros automáticos, etc. Estas señales de alarmas conectan a Carabineros de Chile con las empresas que manejan altas sumas de dinero, a través del sistema Alpha 2 de Carabineros. Desde el 2014 el sistema Alpha III indica una plataforma tecnológica, por medio de la cual, las empresas y la Institución, se vinculan con la finalidad de que las primeras aporten información útil para la toma de desiciones policiales, con ocasión de la activación de alarmas que administren; o con la finalidad de dar aviso de la cancelación de una falsa alarma.

19.1. Elementos utilizados:

Money-Clip (caja registradora): Diseñado para instalarse en cajas registradoras, cajas para dinero y ventanillas de cajeros. Cuando se activa, envía una señal inmediata a la policía o a una oficina central

Pedal de Asalto (mesón de caja): Pedal de atraco pequeño. Ideal para instalar debajo de una mesa.

Pulsador (mesones, baños): El pulsador esta concebido para permitirle separar una llamador telefónico o un controlador personal en forma remota. Puede ser sonoro y/o luminoso o también de forma silenciosa.

Pulsador inalámbrico (vvpp, ggss y bombero de gasolina)

20. Señal de Incendio

Se utiliza para comunicar amagos de incendio, funciona las 24 horas del día protege toda la instalación, sus sensores se encuentran siempre a la vista en los techos al activarse produce sonido. Elementos técnicos usados:

Detector de Humo

- Detector óptico/fotoeléctrico.
- Pueden ser de dos tipos, según detecten el humo por oscurecimiento o por dispersión del aire en un espacio.
- De rayo infrarrojo: están compuestos por un dispositivo emisor y otro receptor. Cuando se oscurece el espacio entre ellos debido al humo.
- De tipo puntual: en ellos, emisor y receptor se encuentran alojados en la misma cámara. Cuando entra humo en la cámara, el haz de luz emitido se refracta en las

partículas de humo y puede alcanzar al receptor, activándose la alarma. Es la tecnología más utilizada en la actualidad.

- De láser: detectan oscurecimiento de una cámara de aglutinación con tecnología láser. Además, dentro de los detectores ópticos/fotoeléctricos, hay dos tipos de tecnologías: detectores análogos y detectores digitales (estas tecnologías se encuentra en los sistemas convencionales y direccionables).
- Detector iónico: Este tipo de detector es más barato que el óptico y puede detectar partículas que son demasiado pequeñas para influir en la luz. Si entra humo en esa cámara se reduce la ionización del aire y la corriente disminuye o incluso se interrumpe, con lo que se activa la alarma El funcionamiento de estos detectores se basa en la disminución de la conductividad del aire.

Detector de Calor

Detector de calor o detector de temperatura es un dispositivo de alarma de incendio diseñado para responder cuando la energía térmica por convección de un incendio aumenta la temperatura de un elemento sensible al calor. Forma parte de un sistemas de detección de incendios.

Detectores Termostáticos: Actúan cuando el elemento detector llega a una temperatura predeterminada. Además de activar una alarma, este dispositivo también se emplea para actuar sobre puertas cortafuegos, persianas o cortinas cortafuegos, compuertas cortafuegos en conductos de ventilación, válvulas de oleoductos, etc. Se fabrican para temperaturas de actuación, entre 70 - 225 ºC.

Detectores Termovelocimétricos: Reaccionan cuando la temperatura aumenta a una velocidad superior a un cierto valor (de 5 a 10 oC por minuto). Estos detectores se basan en la diferencia de respuesta de dos elementos o componentes del dispositivo sensor ante un aumento de temperatura superior a un nivel determinado.

Detectores de Gas: Estos detectores de gases siguen las prescripciones y directrices vigentes en la actualidad relativas a la seguridad propia y se utilizan principalmente para la detección y medición de metano, sulfuro de hidrógeno, monóxido de carbono y oxígeno (también posible otros 50 gases). La función de autocalibración permite una fácil calibración de los medidores de gases. Algunos de ellos poseen la función de almacenamiento y posterior transferencia de los valores de medición a un ordenador.

21. Video Vigilancia Digital

Es una tecnología de vídeo vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades. Es un sistema moderno las cámaras CCTV que se adaptan para poder estar controladas remotamente desde una sala de control, donde se puede configurar su panorámica, inclinación y zoom (PTZ: Pam, Tilt, Zoom. Siglas en Inglés). En efecto, con la video vigilancia digital es posible monitorear remotamente, por medio de Internet, todas las cámaras conectadas a un DVR (Grabador de Video Digital), realizando unas configuraciones según sea la arquitectura de la red. Sin importar cuál sea su proveedor de Internet en todos los casos podemos lograr una adecuada configuración.

Seguridad CCTV Digital Beneficios y Ventajas
Según la instalación y el tamaño de la misma, puede ser más económica una solución digital a una solución IP
Facilidad de uso
Grabación y visualización simultáneas
Mejoras constantes en la tecnología de compresión y el almacenamiento
Alta calidad en la imagen
Alertas automáticas

Ventajas
Se pueden configurar todas las opciones de un sistema IP a un menor precio
Variedad de cámaras y DVRs para diferentes propósitos

22. Video Seguridad con DVR

El DVR es un dispositivo interactivo de grabación de video en formato digital que se utiliza en video seguridad para diversas funcionalidades como el tratamiento de las secuencias de video recibidas, acceso a guías de programación, búsquedas avanzadas de contenidos, conexión a Internet, entre otras.

Características y Ventajas
Equipo diseñado completamente para monitoreo
Nivel de desarrollo más alto que sistemas basados en PC
Si se corta la energía, el DVR vuelve a iniciar automáticamente cuando la energía vuelva sin necesidad de inicio manual
Inmune a virus por carecer de sistema operativo convencional
Monitoreo 24 horas 7 días a la semana
Seguridad en la información guardada

23. Cámaras Domo, IR, PTZ y Cámaras de Seguridad

Las cámaras de seguridad tienen características y funcionalidades que permiten desarrollar la mejor solución para cualquier objetivo. Encontramos cámaras CCTV exteriores, interiores, con visión nocturna, de largo alcance, con visión periférica, con zoom, de alta resolución, cámaras domo, entre muchas otras. En general se pueden encontrar todas las características necesarias para realizar un proyecto personalizado. Es importante realizar un buen diseño teniendo en cuenta todas las características de las cámaras de seguridad, ya que cada una de ellas está diseñada para un fin especifico.

Cámaras IP Fijas
Cámaras IP Domo Fijas
Cámaras IP PTZ
Cámaras IP Domo PTZ
Cámaras IP con Resolución Megapíxel/HDTV
Cámaras IP Térmicas y Cámaras IP para Exteriores

24. Sistema de Video Vigilancia Inteligente IVS

Gracias al sistema de video vigilancia inteligente IVS, ahora podemos tener todas las funcionalidades de las cámaras IP en un sistema vigilancia digital basado en DVR y cámaras CCTV. El sistema es diseñado para aplicaciones donde se necesitan configuraciones muy robustas, y se quiere seguir optando por un sistema de video vigilancia digital-análoga.

Algunas de las características más sobresalientes son
Detección de personas
Contador de objetos
Detección de objetos faltantes
Grabación independiente de video según eventos
Creación de zonas virtuales, si estas son sobrepasadas el DVR nos generara un alerta
Estadísticas de entradas y salidas para mayor seguridad
Ventajas
Variedad de gamas ajustables a diferentes presupuestos
Alta calidad en imagen
Comunicación cerrada hasta el DVR

25. Video Vigilancia IP: Sistemas de Seguridad con Cámaras IP

La video vigilancia IP aprovecha la red informática empresarial sin necesidad de desplegar una infraestructura de cableado coaxial específica para nuestra red de video vigilancia. Así se utiliza el mismo cableado que se emplea para la comunicación de datos, acceso a Internet o correo electrónico. La mayoría de las instalaciones más modernas están abandonando la tecnología analógica en favor de la video vigilancia IP, dada su versatilidad, funcionalidad, sencillez y optimización de las infraestructuras existentes en la compañía.

26. Cámaras IP

Las cámaras de red tienen direcciones IP como cualquier otro dispositivo de red y se pueden instalar con pocos gastos en cualquier parte de la red, siendo controlada centralmente por medio de software. Esto le permite aprovechar la infraestructura existente, como servidores, conmutadores y cableado estructurado, etc. Las cámaras IP pueden ofrecer una resolución hasta 16 veces superior y excelentes capacidades de zoom digital para cubrir un área más amplia. Esto se puede traducir en una mejora en los detalles, como los números de una matrícula, el rostro de una persona o el nombre en la identificación de un empleado. Contamos con una amplia gama de cámaras IP para la video vigilancia profesional. De esta forma podemos satisfacer por completo todas sus necesidades y realizar un diseño adecuado.

Ventajas
Pueden trabajar como cámaras independientes para soluciones pequeñas o integradas entre sí para las soluciones más robustas
Cámaras con inteligencia integrada la cual notifica directamente al NVR o al software de gestión los eventos programados previamente
Bajo costo de instalación
Detección de movimiento
Movimiento direccional
Identificación y movimiento horizontal/vertical/zoom (PTZ)

En aplicaciones de video vigilancia IP, la tecnología inalámbrica es una manera flexible, rentable y rápida de instalar cámaras, especialmente en sistemas IP que cubren áreas de grandes dimensiones, como sistemas de vigilancia para parqueaderos, o el centro de las ciudades. Es una excelente alternativa porque elimina la necesidad de utilizar cables de comunicación. Según las condiciones de la instalación, puede ser conveniente la instalación de red de área local Wireless. Para estos casos contamos con equipos especializados para transmitir inalámbricamente.

Aunque se usa principalmente como un dominio de información pública, Internet puede ser una herramienta muy útil para la video vigilancia. Si se cuenta con las medidas de seguridad correctas como son firewalls, VPN's, entre otros, y se ha implementado la protección por contraseñas y encriptaciones adecuadas, Internet puede también usarse para transferir todos los tipos de información sensible. Actualmente los bancos y otras entidades financieras usan regularmente Internet como un medio para transacciones globales de dinero, emergiendo como un medio probado para otras aplicaciones de seguridad como la vigilancia IP y la monitorización de seguridad. Por eso la importancia de realizar las configuraciones necesarias para la adecuada protección de la transmisión de video por internet.

27. Sistema de Radiocomunicación

Aspectos Reglamentarios: La Subsecretaría de Telecomunicaciones (SUBTEL): es el organismo nacional dependiente del Ministerio de Transporte y Telecomunicaciones, encargado de administrar y reglamentar el uso del espacio radioeléctrico que es compartido por sistemas de comunicaciones públicos y privados. En seguridad se prefieren los equipos VHF, debido a sus condiciones y además permiten el uso de redes y/o sistemas de apoyo complementarios.

Alfabeto Fonético Internacional

Carácter	Palabra	Pronunciación figurada
A	Alfa	Alfa
B	Bravo	Bravo
C	Charlie	Charli
D	Delta	Delta
E	Echo	Eco
F	Foxtrot	Focstrot
G	Golf	Golf
H	Hotel	Jótel o jotél
I	India	India
J	Juliet	Yiuliét
K	Kilo	Kilo
L	Lima	Lima
M	Mike	Maic
N	November	Novemba
O	Oscar	Óscar
P	Papa	Papá or pápa
Q	Quebec	Québec
R	Romeo	Romeo
S	Sierra	Sierra
T	Tango	Tango
U	Uniform	Úniform
V	Victor	Victa
W	Whiskey	Uisqui
X	X-ray	Ecs-rey
Y	Yankee	Yanqui
Z	Zulu	Zulu

FIN MÓDULO 7

SEGURIDAD ELECTRÓNICA

Con esto damos fin a este módulo. Recuerda analizar la información, ejemplos y dinámicas para ponerlas en práctica en tu vida personal y profesional. Ahora puedes realizar el examen.