



## ESCUELA PROFESIONAL DE SEGURIDAD

### *“SUPERVISOR EN SEGURIDAD PRIVADA”*



### MÓDULO:

## SISTEMAS DE ALARMAS Y COMUNICACIONES

## ESTRUCTURA DEL SILABOS DE LA ASIGNATURA

- I. CURSO** : Sistemas de Alarmas y comunicaciones
- II. DESCRIPCION**
- a) Tipos de controles de acceso en tecnología electrónica
  - b) Detección de Intrusión
  - c) Detección de Incendios
  - d) Vigilancia Electrónica
  - e) Centrales de control y dispositivos de señalización
  - f) Centrales de alarmas, campanas electromagnéticas, sirenas electrónicas, balizas, display, pulsadores, alámbricos e inalámbricos.
  - g) Elección de la tecnología para el diseño óptimo de sistemas de seguridad
  - h) El circuito cerrado de televisión. Sistemas de posicionamiento satelital
  - i) El control de alarmas. Los sistemas de control de alarmas. Procedimientos de reacción ante alarmas
  - j) Sistemas de comunicación y enlace. Equipos de comunicación.
  - k) Radiocomunicaciones.
- III. OBJETIVO** : Proporcionar conocimientos al personal de seguridad privada respecto al uso de mecanismos y tecnologías que refuercen las capacidades en cuanto a visión (video sistemas, audición) (diversidad de detectores), olfato (diversidad de detectores), así como información sobre las características de diferentes dispositivos aplicables a la seguridad a fin de cumplir las funciones que la Ley y el reglamento establecen.
- IV. BIBLIOGRAFÍA** : Sistemas de alarmas y comunicaciones – 2019 (systems Perú).

## **Sistema de alarma**

Es un elemento de seguridad pasiva. Esto significa que no evita una intrusión, pero sí es capaz de advertir de ella activando una sirena, cumpliendo así una función disuasiva frente a posibles intrusos. Los equipos de alarma pueden estar conectados con una central perceptora o monitoria, a través del teléfono, radio, celular, internet, etc.



### **a. Tipos de controles de acceso en tecnología electrónica**

Los sistemas de control de acceso regulan la entrada de personas a cualquier recinto y lugar. El control de accesos se emplea para evitar que personas no autorizadas o deseadas tengan acceso a un lugar en particular. A lo largo del tiempo, se han venido utilizando controles de acceso físicos a través de vigilantes y personal de seguridad, pero hoy en día, son de tipo electrónico y se controla de una forma mucho más sofisticada y segura.

Para lograr dicha función, un terminal para el control de accesos electrónicos cuenta con un lector que puede analizar una tarjeta, una clave y hasta una cualidad física (a través de biometría) por huella, proximidad, iris, palma mano, etc... Después, el sistema verifica si la información analizada está en su base de datos y si es así; la persona puede acceder al recinto o lugar.

Los sistemas de control de acceso electrónicos se han hecho muy populares en empresas e instituciones que venían utilizando los sistemas de control de accesos con personal, además, al ser su precio cada vez más asequible, también están siendo implantados en domicilios particulares y residencia.

“Un control de acceso electrónico es una solución efectiva, económica y simple; y evita que personas no autorizadas accedan a los lugares donde están instalados”.

Los sistemas de control de acceso regulan la entrada de personas a cualquier recinto y lugar.

El control de accesos se emplea para evitar que personas no autorizadas o deseadas tengan acceso a un lugar en particular. A lo largo del tiempo, se han venido utilizando controles de acceso físicos a través de vigilantes y personal de seguridad, pero hoy en día, son de tipo electrónico y se controla de una forma mucho más sofisticada y segura.

Para lograr dicha función, un terminal para el control de accesos electrónicos cuenta con:

- Lector que puede analizar una tarjeta
- Lector en el cual se introduzca una clave.
- Lector de hasta una cualidad física (a través de la biometría) por huella digital, proximidad del iris, palma de la mano, etc.



Después, el sistema verifica si la información analizada está en su base de datos y si es así; la persona puede acceder al recinto o lugar.

**Los sistemas de control de acceso electrónicos** se han hecho muy populares en empresas e instituciones que venían utilizando los sistemas de control de accesos con personal, además, al ser su precio cada vez más

asequible, también están siendo implantados en domicilios particulares y residencia.

“Un control de acceso electrónico es una solución efectiva, económica y simple; y evita que personas no autorizadas accedan a los lugares donde están instalados”.

### **Tipos de controles de acceso electrónicos**

Tipos de controles de acceso en tecnología electrónica son:

Autónomas y Lectoras

Se sub dividen en:

- Control de acceso autónomo Biométrico
- Control de acceso autónomo de proximidad
- Control de asistencias y Software, se sub divide en:
  - ✓ Biostation
  - ✓ Biolite net
  - ✓ Software S.C.A.T SAC500
  - ✓ Control de acceso a la medida.
- Lector Biométrico USB



#### **- Sistemas biométricos**

Los controles de acceso biométricos consisten en la identificación de personas mediante una o varias características físicas. Los sistemas de control de accesos y presencia más utilizados son: reconocimiento del

rostro (facial), por el iris, de reconocimiento de voz, de retina, reconocimiento de palma de la mano y por la firma. Listamos aquí los sistemas de control de acceso biométrico que más se están implantando y que son ofrecidos por las principales compañías y dirigidos tanto a grandes empresas como a Pymes para que puedas elegir el mejor terminal para el control de accesos biométricos.

#### - **Control de Accesos Edificios**

Mejores Sistemas Control de Accesos Edificios: Empresas que ofrecen distintos sistemas de seguridad para el control de accesos en edificios.

**Cerraduras sin llaves – Cerradura teléfono móvil, Abrir puerta con teléfono móvil Bluekey y Simons – Voss.**

Un nuevo tipo de cerraduras están causando la revolución en cuanto a la seguridad y el control de accesos a la vivienda se refiere. Estas son las nuevas cerraduras sin llaves que funcionan con un teléfono móvil a través de Bluetooth y que son capaces de abrir cualquier puerta de forma automática gracias a la tecnología combinada que ofrecen Bluekey y Simons-Voss.

Sin ninguna instalación ni llaves, tan sólo cambiando el pomo podremos olvidarnos de las llaves y podremos abrir con el mismo teléfono las puertas de la oficina, de casa., de nuestro parking, etc.

#### - **Control de Accesos en Viviendas**

Mejores Sistemas Control de Accesos en Viviendas: Descubre lo último que se está utilizando para el control de accesos en viviendas.

Domótica para Viviendas, Hogar Digital, Viviendas Inteligentes Domótica Hogar Digital



Cerraduras sin llaves – Cerradura teléfono móvil, Abrir puerta con teléfono móvil Bluekey y Simons-Voss

Un nuevo tipo de cerraduras están causando la revolución en cuanto a la seguridad y el control de accesos a la vivienda se refiere. Estas son las nuevas cerraduras sin llaves que funcionan con un teléfono móvil a través de Bluetooth y que son capaces de abrir cualquier puerta de forma automática gracias a la tecnología combinada que ofrecen Bluekey y Simons-Voss.

Sin ninguna instalación ni llaves, tan sólo cambiando el pomo podremos olvidarnos de las llaves y podremos abrir con el mismo teléfono las puertas de la oficina, de casa., de nuestro parking, etc.

- **Control de Accesos Hoteles**

Mejores Sistemas Control de Accesos Hoteles: Empresas especializadas en la implantación de sistemas para el control de acceso en hoteles y la seguridad.



- **Control de Acceso Inalámbrico para Hoteles**

Listado de compañías especializadas en la implantación de sistemas para el Control de Acceso en Hoteles y la seguridad:

- **Control de Accesos Hoteles de Simonalert**

SimonAlert ofrece soluciones para el perfecto control de entradas y salidas en hoteles con supervisión desde la recepción. Disuade el acceso de personas ajenas al hotel. Ver Solución SimonAlert.

- **Control de Accesos Hoteles de inhova**

INHOVA ofrece un sistema integral para el control de accesos en hoteles: Sistemas y cerraduras, equipos de gestión, lectores murales, cajas fuertes, des conectores de energía, periféricos Check In/Out y planes de accesos. Ver Soluciones Inhova

- **Control de Accesos para Hoteles de kaba**

Kaba empresa reconocida en el sector ofrece una amplia gama de soluciones para el control de accesos y la seguridad en Hoteles. Sus soluciones aumentan la seguridad del huésped, optimizan la gestión de empleados e incrementan la productividad. Ver soluciones Kaba

- **Control de Accesos Oficinas**

Mejores Sistemas Control de Accesos Oficinas: Compañías que ofrecen soluciones y software para el control de accesos y la seguridad en oficinas.



Cerraduras sin llaves – Cerradura teléfono móvil, Abrir puerta con teléfono móvil Bluekey y Simons-Voss.

Listado de Compañías que ofrecen soluciones para el control de accesos y la seguridad en oficinas.

- **Control de Accesos Oficinas de Tecoyse**

TECOYSE, S.L. ofrece soluciones para el control de acceso a la oficina mediante lector de huella dactilar con registro de fecha, hora y usuario, según horarios establecidos, etc. Ver Soluciones TECOYSE

- **Control de Accesos Parkings y Garajes**

Mejores Sistemas Control de Accesos Parkings y Garajes: Empresas que ofrecen diferentes sistemas para el control de accesos en parkings y garajes de comunidades y empresas.

Listado de empresas que ofrecen sistemas para el control de acceso y la seguridad en parkings y garajes.

- **Control de Accesos a Parkings y Garajes de Accesor**

Accesor ofrece una amplia gama de soluciones para el control de acceso a parkings y garajes. Ver soluciones Accesor

- **Control de Accesos a Parkings Comunitarios de kimaldi**

Kimaldi ofrece la solución KTRANSINT idónea para parking comunitarios muy útil cuando hay plazas de parking compartidas o alquiladas por horas.

- **Control de Accesos Por Huella**

Mejores Sistemas Control de Accesos Por Huella: Terminales para el control de acceso por huella dactilar ofrecidos por las principales empresas. Compara precios y características.



- ✓ Control de empleados
- ✓ Control de errantes
- ✓ Control de personal
- ✓ Control de presencia
- ✓ Control de producción
- ✓ Control de recinto deportivo
- ✓ Domótica
- ✓ Control de acceso de Empresas
- ✓ Lectoras de proximidad RFID, magnéticos y tarjeta
- ✓ Tornos de acceso
- ✓ Sistemas de Identificación

El control de Acceso, basada principalmente en las áreas de detección de incendio, sistemas de video, controles de acceso y detección de intrusos.

Son cada vez más numerosas las empresas que necesitan ejercer control sobre el ingreso y egreso de personas a su lugar de trabajo, o limitar, cuántos y quienes ingresan a un determinado lugar.

Una de las formas de implementarlo es instalar un control de acceso por tarjetas de proximidad, banda magnética, etc. Que, conectados a un sistema computarizado permite además de controlar el acceso, establecer el horario de trabajo, tener estadísticas, conocer los nombres y el tiempo que una determinada persona permanece en un lugar, etc.

Estos sistemas, complementan la seguridad de inmuebles en general, aunque son más utilizados en empresa de todo tipo.

Consiste básicamente en LECTORES de distintos formatos, los que permiten, eléctricamente la apertura de puertas exteriores e interiores, a través de tarjetas magnéticas, código de barras, de proximidad, y otras de mayor sofisticación y tecnología.

Todo el sistema eléctrico – electrónico está acompañado por un SOFTWARE de gestión para control de accesos y de personal, reportado las novedades y administrando las mismas para un control estricto de todos y cada uno de los ingresos y egresos que se produjeron, no accediendo a las aperturas e ingresos por personal no autorizado ni dado de alta en el sistema.

## b. Detección de Intrusión

Acción de introducirse sin derecho en un dignidad, jurisdicción, oficio, etc.; se aplica específicamente al ejercicio indebido de las profesiones y es castigado por el Código Penal.

Sinónimos: Intromisión, entremetiendo, entrometiendo, irrupción, invasión, incursión, entrada.

Los Sistemas de Intrusión/Robo o Alarma de Intrusión, son aquellas herramientas electrónicas que protegen a los inmuebles, los bienes y los inquilinos de una vivienda o edificio. Se puede crear con las Alarmas de Intrusión una protección de varios niveles como protección exterior, perimetral, inferior, robo y alarma de asalto.

Un sistema de alarma de intrusión es un elemento de seguridad pasiva. Esto significa que no evitan una intrusión, pero sí capaces de advertir de ella, cumpliendo así, una función disuasoria frente a posibles intrusos y los avisos a los propietarios y los agente de seguridad necesarios.



Niveles de Seguridad para las Alarmas de Intrusión:

Las alarmas de intrusión se definen en distintos niveles. A continuación se explicará cada uno de los niveles de protección de alarmas de seguridad de intrusión desde fuera hacia dentro:

## 1. Protección Exterior

La protección Exterior tiene como objetivo detectar presencia de objetos, personas, vehículos, etc., en la parte exterior del inmueble. Dependiendo de la tipología del edificio se utilizan distintas soluciones tecnológicas, pero algunas de los más comunes son:

- Barreras de rayos infrarrojos, microondas, láser, etc., que crean una barrera o volumen protegido invisible.
- Detectores de movimiento exteriores que detectan el movimiento de vehículos o personas en el exterior.
- Detectores enterrados que han sido diseñados para la instalación bajo tierra y pueden detectar tanto la presión generada por personas o vehículos sobre tierra, como movimientos subterráneos, por máquinas o personas.
- Detección subacuática que detecta presencia de barcos, vehículos y buceadores con acceso por agua.
- Detección aérea que detecta el acceso de vehículos o personas que acceden por aire.
- Protección Perimetral – La protección perimetral hace referencia a soluciones que avisan sobre el intento de intrusión en el mismo edificio. Las protecciones perimetrales más comunes son:
  - Detectores de Apertura de Puertas y Ventanas que avisan si se abre una puerta o ventana
  - Barreras de rayos infrarrojos que avisan si se detecta la introducción de algún objeto o persona por algún hueco, como una ventana abierta, puerta, etc.



- Sensores de sonido, que tienen como objetivo avisar si se rompe un ventana, produce un sonido fuerte, etc., qué puede ser una indicación de que se está produciendo un intento de intrusión.
- Sensores sísmicos, que tienen como objetivo avisar de si se está produciendo algún intento de acceso para una pared, suelo o techo de inmueble.

## 2. Protección Interior

La protección de interior, detecta una intrusión dentro de la misma vivienda. Los sistemas más comunes son:

- Detectores de Movimiento o Presencia, que detectan la presencia o el movimiento dentro del inmueble.
- Barreras de rayos infrarrojos, microondas, láser, etc., que crean una barrera o volumen protegido invisible.
- Protección de Objetos – la protección de objetos se centra en objetos de valor, como cajas, fuertes, cuadros, esculturas, etc. Normalmente se protegen estos elementos con:
  - Detectores de Robo de detectan cuando un objeto se traslada.
  - Detectores sísmicos que detectan golpes o movimientos en paredes, protecciones de cristal, etc., que están alrededor de caja fuertes u obras de arte, etc.
  - Barreras infrarrojos, que avisan si alguien o algo intentan acercarse a un objeto.

### Sistemas de detección de intrusiones

El término IDS (Sistema de detección de intrusiones) hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Existen dos claras familias importantes de IDS:

- El grupo N – IDS (Sistema de detección de intrusiones de red), que garantiza la seguridad dentro de la red.
- El grupo H – IDS (Sistema de detección de intrusiones en el host), que garantiza la seguridad en el host.

Un N – IDS necesita un hardware exclusivo. Éste forma un sistema que puede verificar paquetes de información que viajan por una o más líneas de la red para descubrir si se ha producido alguna actividad maliciosa o anormal. El N – IDS pone uno más de los adaptadores de red exclusivos del sistema en modo promiscuo. Este es una especie de modo “invisible” en el que no tienen dirección IP. Tampoco tienen una serie de protocolos asignados. Es común encontrar diversos IDS en diferentes partes de la red. Por lo general, se colocan sondas fuera de la red para estudiar los posibles ataques, así como también se colocan sondas internas para analizar solicitudes que hayan pasado a través del firewall o que se han realizado desde dentro.

### **Técnicas de detección**

El tráfico en la red (en todo caso, en Internet) generalmente está compuesto por datagramas de IP. Un n – IDS puede capturar paquetes mientras estos viajan a través de la conexiones físicas a las que está sujeto. Un N – IDS contiene una lista TCP/IP que se asemeja a los datagramas de IP y a las conexiones TCP. Puede aplicar las siguientes técnicas para detectar intrusiones.

Verificación de la lista de protocolos: Algunas formas de intrusión, como “Ping de la muerte” y “escaneo silencioso TCP” utilizan violaciones de los protocolos IP, TCP, UDP e ICMP para atacar un equipo. Una simple verificación del protocolo puede revelar paquetes no válidos e indicar esta táctica comúnmente utilizada.

### **Verificación de los protocolos de la capa de aplicación:**

Algunas formas de intrusión emplean comportamientos de protocolos no válidos, como “WinNuke”, que utiliza datos NetBIOS no válidos (al agregar datos fuera de la banda). Para detectar eficazmente estas intrusiones, un N IDS debe haber implementado una amplia variedad de protocolos de la capa de aplicación, como NetBIOS, TCP/IP, etc.

Esta técnica es rápida (el N – IDS no necesita examinar la base de datos de firmas en su totalidad para secuencias de bytes particulares) y es también más eficiente, ya que elimina algunas Falsas alarmas. Por ejemplo, el analizar protocolos, N – IDS puede diferenciar un “Back Oríifice PING” (bajo peligro) de un “Back Oríifice COMPROMISE” (alto peligro).

## Reconocimiento de ataques de “comparación de patrones”

Esta técnica de reconocimiento de intrusión es el método más antiguo de análisis N – IDS y todavía es de uso frecuente.

Consiste en la identificación de una intrusión al examinar un paquete y reconocer, dentro de una serie de bytes, la secuencia que corresponde a una firma específica. Por ejemplo, al buscar la cadena de caracteres “cgi – bin/pht”, se muestra un intento de sacar provecho de un defecto del script CGI “pht”. Este método también se utiliza como complemento de los filtros en direcciones IP, en destinatarios utilizados por conexiones y puertos de origen y/o destino. Este método de reconocimiento también se puede refinar si se combina con una sucesión o combinación de indicadores TCP.

Esta táctica está difundida por los grupos N – IDS “Network Grep”, que se basan en la captura de paquetes originales dentro de una conexión supervisada y en su posterior comparación al utilizar un analizador de “expresiones regulares”. Éste intentará hacer coincidir las secuencias en la base de firmas byte con el contenido del paquete capturado.

La ventaja principal de esta técnica radica en la facilidad de actualización y también en la gran cantidad de firmas que se encuentran en la base N – IDS. Sin embargo, cantidad no siempre significa calidad. Por ejemplo, los 8 bytes “CE63D1D2 16E713CF”, cuando se colocan al inicio de una transferencia de datos UDP, indican un tráfico Back Orifice con una contraseña predeterminada. Aunque el 80% de las intrusiones utilicen la contraseña predeterminada, el 20% utilizarán contraseñas personalizadas y no serán necesariamente reconocidas por el N – IDS. Por ejemplo, si la contraseña se cambia a “evadir”, la serie de bytes se convertirá en “8E422A52C 0666BC4A”, lo que automáticamente la protegerá que el N – IDS la capture.

Además, la técnica inevitablemente conducirá a un gran número de falsas alarmas y falsos positivos.

Existen otros métodos para detectar e informar sobre intrusiones, como el método Patten Matching Stateful, y/o para controlar el tráfico peligroso o anormal en la red.

En conclusión, un perfecto N – IDS es un sistema que utiliza las mejores partes de todas las técnicas mencionadas anteriormente.

### **Qué hacen los IDS**

Los principales métodos utilizados por N – IDS para informar y bloquear intrusiones son:

- Reconfiguración de dispositivos externos (firewalls o ACL en routers): Comando enviado por el N – IDS a un dispositivo externo (como un filtro de paquetes o un firewall) para que se reconfigure inmediatamente y así puede bloquear una intrusión. Esta reconfiguración es posible a través del envío de datos que expliquen la alerta (en el encabezado del paquete).
- Envío de una trampa SNMP a un hipervisor externo: Envío de una alerta (y detalles de los datos involucrados) en forma de un datagrama SNMP a una consola externa como HP Open View Tivoli, Cabletron, Spectrum, etc.
- Envío de un correo electrónico a uno o más usuarios: Envío de un correo electrónico a uno o más buzones de correo para informar sobre una intrusión seria.
- Registro del ataque: Se guardan los detalles de la alerta en una base de datos central, incluyendo información como el registro de fecha, la dirección IP del intruso, la dirección IP del destino, el protocolo utilizado y la carga útil.
- Almacenamiento de paquetes sospechosos: Se guardan todos los paquetes originales capturados y/o los paquetes que dispararon la alerta.
- Apertura de una aplicación: Se lanza un programa externo que realice una acción específica (envío de un mensaje de texto SMS o la emisión de una alarma sonora)
- Envío de un “Resetkill”: Se construye un paquete de alerta TCP para forzar la finalización de una conexión (sólo válidos para técnicas de intrusión que utilizan el protocolo de transporte TCP)
- Notificación visual de una alerta: Se muestra una alerta en una o más de las consolas de administración.

## PROCEDIMIENTO DE REACCIÓN EN CASO DE UN EVENTO DE INTRUSIÓN.

- (1) SE RECIBE UNA SEÑAL POR LA EMPRESA DE MONITOREO SE GENERAN SEÑALES DE INTRUSIÓN POR EL SISTEMA DE SEGURIDAD.
- (2) SE COMUNICA CON EL ENCARGADO DE LA DEPENDENCIA PARA CONFIRMAR EL EVENTO
  - (2-1) EL SUPERVISOR HACE LA VERIFICCIÓN DE EVENTO
  - (2-2) SE CONFIRMA UN EVENTO DE INTRUSIÓN
  - (2-3) SE CONFIRMA UN EVENTO DE FALSA ALARMA
- (3) SE DESPACHA PRIMERA RESPUESTA DE PARTE DEL SUPERVISOR DE LA EMPRESA DE MONITOREO.
- (4) EL SUPERVISOR SE COMUNICA CON LA EMPRESA DE MONITOREO. LA EMPRESA DE MONITOREO INFORMA LO VERIFICADO A LA SCRR.

EL SUPERVISOR LLAMA A LA CENTRAL DE LA EMPRESA DE MONITOREO

DEJA UN VOLANTE DE EVIDENCIA DE LA VISTA 3-4

\*COMUNICARSE VÍA CELULAR O FIJO CON LA DEPENDENCIA.

### **Detección de Intrusión**

#### **Sistemas de detección de intrusiones**

El término IDS (Sistema de detección de intrusiones) hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la res para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Existen dos claras familias importantes de IDS:

El grupo N – IDS (Sistema de detección de intrusiones de red), que garantiza la seguridad dentro de la red.

El grupo H – IDS (Sistema de detección de intrusiones en el host), que garantiza la seguridad en el host.

Un N – IDS necesita un hardware exclusivo. Éste forma un sistema que puede verificar paquetes de información que viajan por una o más líneas de la red para descubrir si se ha producido alguna actividad maliciosa o anormal. El N – IDS pone uno o más de los adaptadores de red exclusivos del sistema de modo promiscuo. Éste es una especie de modo “invisible” en el que no tienen dirección IP. Tampoco tienen una serie de protocolos asignados. Es común encontrarse diversos IDS en diferentes partes de la red. Por lo general, se colocan sondas fuera de la red para estudiar los posibles ataques, así como también se colocan sondas internas para analizar solicitudes que hayan pasado a través de firewall o que se han realizado desde adentro.

### **Técnicas de detección**

El tráfico en la red (en todo caso, en internet) generalmente está compuesto por datagramas de IP. Un N – IDS puede capturar paquetes mientras estos viajan a través de las conexiones físicas a las que está sujeto. Un N – IDS contiene una lista TCP/IP que se asemeja a los datagramas de IP y las conexiones TCP. Puede aplicar las siguientes técnicas para detectar intrusiones.

Verificación de la lista de protocolos. Algunas formas de intrusión, como “Ping de la muerte” y “escaneo silencioso TCP” utilizan violaciones de los protocolos IP, TCP, UDP e ICMP para atacar un equipo. Una simple verificación del protocolo puede revelar paquetes no válidos e indicar esta táctica comúnmente utilizada,

### **c. Detección de incendios**

Estos sistemas permiten la detección temprana de un principio de incendio, a través de detectores especiales que permiten censar la existencia de una abrupta elevación de temperatura o la existencia de humo, paso previo de una combustión que puede generar un incendio de magnitudes importantes.

Básicamente consiste en una central inteligente que de acuerdo a las señales eléctricas provenientes de detectores especialmente diseñados, permite dar una respuesta acústica y/o lumínica emanada de los detectores automáticos o

de detectores manuales, activando sirenas de emergencia o activando actuadores que permitirán reducir los efectos de llamas o temperaturas, hasta la extinción por personal idóneo, entrenado a tal efecto.



En la vida moderna, es imprescindible que cada nuevo emprendimiento edilicio, cuente con un sistema de detección de incendio, que permita identificar la ubicación de cualquier foco de incendio cuando todavía es fácil de sofocar.

Esto no solo es norma en las grandes construcciones, sino que a nivel familiar, son cada vez más numerosas las casas que cuentan con algún tipo de sensor en las partes más delicadas de la casa, como por ejemplo la cocina.

Desde los más simples sistema de detección, que van adosados a una central de alarma domiciliaria, hasta grandes sistemas direccionales y analógicos que permiten identificar el lugar donde se produce una sobre temperatura o cantidades de humo que hagan presumir un foco de incendio, o permitan conocer el nivel de contaminación de cada sensor y cuando alguno de éstos ha salido de servicio, se han implementado en una instalación.

## Detector de Humo



Un detector de humo es un aparato de seguridad que detecta la presencia de humo en el aire y emite una señal acústica avisando del peligro de incendio. Atendiendo al método de detección que usan pueden ser de varios tipos: - Detectores iónicos: Utilizados para la detección de gases y humos de combustión que no son visibles a simple vista. - Detectores de humos: Detectan los humos visibles mediante la absorción o difusión de la luz.

Pueden ser de dos tipos, según detecten el humo por oscurecimiento o por dispersión del aire en un espacio:

- De rayo infrarrojo, compuestos por un dispositivo emisor y otro receptor. Cuando se oscurece el espacio entre ellos debido al humo sólo una fracción de la luz emitida alcanza al receptor provocando que la señal eléctrica producida por éste sea más débil y se active la alarma.
- De tipo puntual, en los que emisor y receptor se encuentran alojados en la misma cámara pero no se ven al formar sus ejes un ángulo mayor de  $90^\circ$  y estar separados por una pantalla, de manera que el rayo emitido no alcanza el receptor. 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.

### **d. Vigilancia electrónica**

Se entiende como “Vigilancia electrónica” la utilización de todos los medios tecnológicos y/o electrónicos, con la finalidad de acopiar información y pruebas

respecto a la comisión del delito en estudio o la responsabilidad penal de sus autores.

La vigilancia es el monitoreo del comportamiento. La vigilancia por sistema es el proceso de monitoreo de personas, objetos o procesos dentro de sistemas para la conformidad de normas esperadas o deseadas en sistemas confiables para control de seguridad o social.

A pesar de que en francés la palabra vigilancia significa literalmente “mirar por encima”, el término vigilancia suele aplicarse a toda forma de observación o monitoreo, no sólo la observación visual.

Sin embargo, el “ojo en el cielo” que todo lo ve es aún el icono de la vigilancia. Para la vigilancia en muchas ciudades modernas y edificios se suelen emplear circuitos cerrados de televisión. Si bien la vigilancia puede ser una herramienta útil para las fuerzas y empresas de seguridad, mucha gente se muestra preocupada por el tema de la pérdida de privacidad.

La palabra vigilancia suele usarse para describir la observación desde una distancia por medio de equipo electrónico u otros medios tecnológicos. Estos equipos electrónicos pueden ser:

- Escuchas telefónicas
- Aparatos de escucha encubiertos
- Micro cámaras
- Circuitos cerrados de televisión
- Rastreo GPS
- Imágenes CCTV
- Vigilancia por computadora e internet.

Es el control y seguimiento de la seguridad física y electrónica, que son el conjunto de recursos humanos, tecnológicos y operacionales, que tienen como propósito resguardar la vida, bienes, operación e información de las organizaciones, contra eventos o actos negativos no deseados.

Esta vigilancia lo lleva a cabo personal especializado y capacitado en Seguridad electrónica y control de instrumentos de medición o alarma conformada por un conjunto de dispositivos electrónicos instalados estratégicamente y diseñados para el registro de diferentes tipos de eventos,

detectar cambios de variables físicas como son: movimiento, sonidos, gases o humos, calor, infrarrojos etc. La información capturada es almacenada y analizada, para la toma de acciones que mitiguen o combatan las acciones de riesgo detectados.

Las computadoras pueden ser vigiladas por diversos métodos, desde la instalación de dispositivos físicos de escucha al software de vigilancia a la interceptación remota de las transmisiones de radio generadas por su normal funcionamiento.

El spyware, término acuñado por el experto en seguridad informática Steve Gibson, se suele usar para describir las herramientas de vigilancia informáticas que se instalan en contra de los deseos del usuario. Las conexiones de banda ancha a internet han hecho a las computadoras más vulnerables que hasta ahora.

El uso de escucha telefónicas oficiales y no oficiales se ha hecho común. Prueba de ello es que la Agencia de Seguridad Nacional de los Estados Unidos se dedica a interceptar, almacenar y analizar – con y sin órdenes judiciales – las conversaciones telefónicas de los habitantes de EUA.

Los contratos o licencias por medio de las cuales el estado controla a las compañías telefónicas incluyen cláusulas para que den acceso para realizar escuchar telefónicas a las fuerzas de seguridad y la policía. La vigilancia aplicada a teléfonos celulares consiste en el almacenamiento de datos que incluyen información sobre el tiempo de duración de llamadas, emisor y lugar de realización. Actualmente los métodos de vigilancia de telefonía celular incluyen no sólo la ubicación o almacenamiento de datos de la llamada, considerando que en los últimos años han surgido una infinidad de spyware en el teléfono móvil que permiten el rastreo, grabar llamadas, interceptar, desviar, bloquear, leer SMS y correo electrónico.

## **e. Centrales de control y dispositivos de señalización**

### **Centrales de control**

El Centro de Control es un ambiente seleccionado dentro de las instalaciones de una empresa o institución que está a cargo de un grupo de operadores que se encargan de mantener un constante enlace, coordinación, supervisión y control por medios radiales y/o electrónicos con los elementos de seguridad o sistemas electrónicos de seguridad.

Una vez organizado el Centro de control, se debe formular un plan de reacción inmediata como parte del plan general de seguridad integral.

Solo la centralización de la información y su acceso inmediato en tiempo real permiten el control absoluto de una operación proveen la valiosa oportunidad de tomar decisiones acertadas en el menor tiempo posible, asegurando el éxito de procesos operaciones.

Los centrales o paneles de alarma los cuales son el “cerebro” de todo el sistema ya que actúan sobre él todas las señales eléctricas de los distintos bloques, actuando en consecuencia.

De acuerdo al tipo de inmueble a proteger y a las características de la zona, los paneles se clasifican en ALAMBRICOS E INALAMBRICOS, ya sea que requieran o no cables para la interconexión de los dispositivos involucrados en la instalación (recordemos que estos sistemas eléctricos – electrónicos son de baja tensión, ya que trabajan con voltajes de 12 volts de corriente continua). Asimismo y de acuerdo a las dimensiones del sector a proteger, encontramos en el mercado PANELES de 4,8 o 16 zonas, micro procesado, pudiendo obtener más zonas con expansores de zona.

**ZONA DE UN PANEL:** Es el lugar físico donde se conectan DETECTORES dentro de un papel de control y por ende dentro de la instalación en general.

Este bloque lo constituyen los distintos dispositivos que permitirán DETCTAR UN EVENTO (intrusión, rotura de vidrio, pasos indebidos, apertura de puertas o ventanas, escape de gases tóxicos, etc.) Cada DETCTOR está diseñado para enviar una señal eléctrica o a la central o panel, el que actuará en consecuencia dando.

## **SEÑAL DE ALARMA**

Los detectores más utilizados en estos sistemas de seguridad son los siguientes

- Detectores magnéticos de apertura de puertas y ventanas.
- Detectores de rotura de vidrios y cristales
- Detectores de movimiento por infrarrojo pasivo
- Barreras infrarrojas
- Detectores de doble Tecnología
- Detectores de humo: Fotoeléctrico o Iónicos.

## Dispositivos de señalización

El aviso de evento ocurrido 8 asaltos, robo, incendio, etc., es tan importante como la selección de los detectores que permitirán captar un evento indeseado.

Normalmente un evento se señala de forma acústica (a través de la sonorización de sirenas, bocinas o campanas, de distintas potencias y niveles acústicos) como así también con sistemas lumínicos 8 lámparas, flashes, etc.) O combinación de ambos.

El método de señalización más eficiente y que acompaña siempre a los anterior es el de MONITOREO de alarmas vía telefónica, radial o internet. Este sistema consiste en el envío de una señal por alguna de la vías indicadas a un Estación Central de monitoreo, encargada de “monitorear” todas los sistemas conectados a su red y actuar en consecuencia, dándoles inmediato aviso a la policía, bomberos, ambulancias, usuarios, etc. O bien donde el usuario haya dejado sus directivas en caso de eventos de esa naturaleza. Las estaciones de monitoreo están preparadas con personal idóneo para dar respuesta inmediata y así minimizar los riesgos.

### **f. Centrales de alarmas, campanas electromagnéticas, sirenas electrónicas, balizas, display, campanas e inalámbricos**

#### Centrales de alarmas

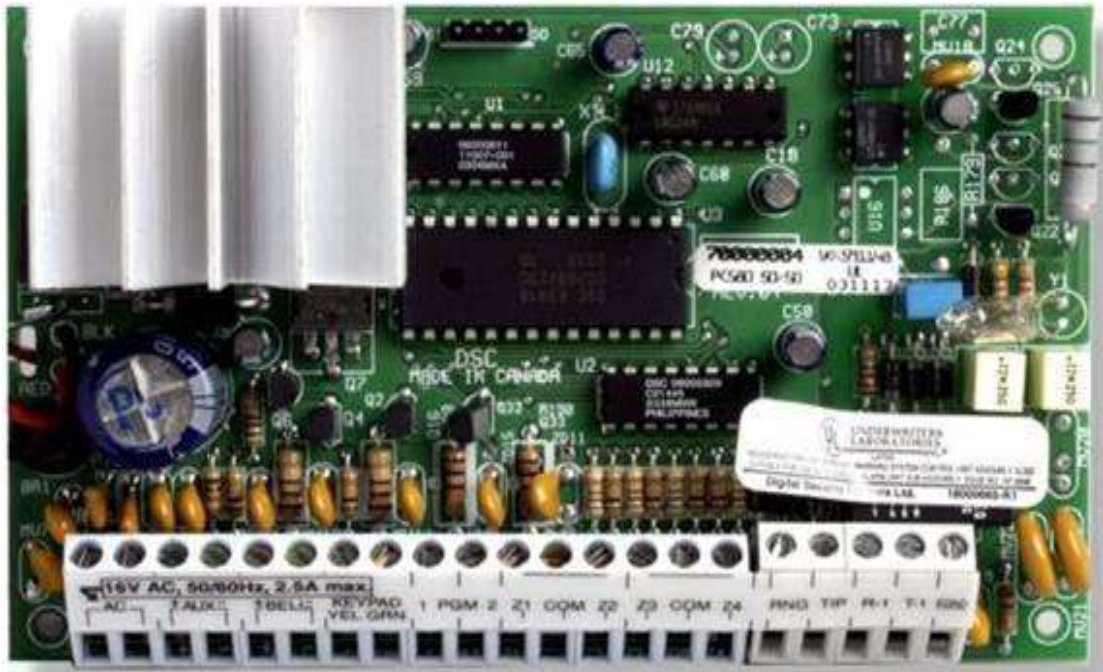
##### Central de Alarma

La central de alarma es el cerebro de todo el sistema, posee un microprocesador que es encargado, de acuerdo a su programación, de recibir las señales de los sensores y tomar acciones como activar una sirena, un emisor telefónico, etc. La central dispone de un cargador automático para batería que será la encargada de alimentar a todo el sistema en caso de corte del suministro eléctrico.

##### Central procesadora.

Es la CPU del sistema. En ella se albergan la placa base, la fuente y la memoria central.

Esta parte del sistema es la que recibe las diferentes señales que los diferentes sensores pueden emitir, y actúa en consecuencia, disparando la alarma, comunicándose con la central por medio de un modem, etc. Se alimenta a través de corriente alterna y de una batería respiratoria, que en caso de corte de la energía, le proporcionaría una autonomía al sistema de entre 12 horas y 3 días (dependiendo de la capacidad de la batería).



Los modelos disponibles de centrales, parten de una base de 4 zonas y existen modelos hasta 128 zonas. Los modelos multiplexados (Particiones) permiten a partir de cuatro cables particional una central de alarma funcionando la misma como si fueran dos o cuatro centrales independientes.

Los mejores dispositivos y las mejores marcas que se adaptan a cualquier necesidad como en:

- Oficinas
- Bodegas
- Industrias
- Comercios

## **Generador de Niebla**

Generador de Niebla que en poco segundos llena la estancia con una densa e inofensiva Niebla de Seguridad de tal forma que el ladrón le resulte imposible ver su propia mano frente a la cara.

Es un dispositivo de seguridad adaptable al panel de Alarma que permite en pocos segundos llenar la estancia con una densa e inofensiva Niebla de Seguridad de tal forma que al ladrón le resulte imposible ver su propia mano frente a la cara, monitoreado a través de nuestra central.

## **Verificación y Rondines**

Monitoreo de Alarmas

Verificación de eventos con bases y rondines en la periferia de sus instalaciones gracias a nuestras unidades móviles.

Tener cerca una unidad de verificación persuade a los delincuentes de cometer algún delito, es por eso que te ofrecemos los servicios bases y rondines en la periferia de tus instalaciones.

## **Cerca Electrificada**

Monitoreo de Alarmas

Cerca electrificada con 12,500 voltios de carga eléctrica en pulsaciones, monitoreada por nuestra central de monitoreo.

## **PROTECCIÓN PERIMETRAL**

Cuenta con 12,500 voltios de carga eléctrica en pulsaciones

El gasto de electricidad equivale a 1 foco de 40 watts.

La cerca queda monitoreada por nuestra central de monitoreo.

## **Circuito Cerrado de Televisión**

Monitoreo de Alarmas

Circuito cerrado de televisión adaptable al ramo industrial, comercial, residencial, y al sector público con capacidad de monitoreo remoto.

Es un sistema electrónico compuesto por Cámaras, monitores, DVR o TVR que almacenan la grabación y ayudan a supervisar puntos estratégicos o de alta seguridad de alguna propiedad con capacidad de monitoreo remoto.

La manera más eficiente para saber qué es lo que está pasando, aplicado en:

- Ramo industrial
- Ramo comercial
- Residencial
- Sector Público

### **Emergencia Médica**

Monitoreo de Alarmas

Se activa el botón de Emergencia Médica en el teclado y se solicitan los datos de su médico, estos se almacenan junto con toda la información del cliente para algún caso de emergencia.

### **Control de Acceso**

Monitoreo de Alarmas

Control de acceso con sistemas electrónicas que le permiten sentirse seguro al momento de controlar quienes entran a su hábitat, gracias a la facilidad de instalación de los dispositivos en diferentes puntos.

Un control de accesos surge de la necesidad de proteger las instalaciones mediante barreras físicas operadas por un proceso automatizado, centrándose en las personas, los vehículos que los trasladan y los objetos que porten o transporten.

En la actualidad las empresas, tanto a nivel nacional como a nivel internacional, encuentran entre sus prioridades más inmediatas la de ejercer, de manera óptima y eficaz, un control de acceso en sus instalaciones. Por otra parte, también es importante la utilización de esos sistemas para supervisar el horario de llegada y salida de empleados, así como autorizar o denegar acceso a intrusos.

### **Detección y extinción incendios**

Monitoreo de Alarmas

Detección de incendios con sistemas inteligentes como la extinción a base de agua o con agentes limpios, la alarma de incendio y voceo digital, los sensores de flama o gas y los de monóxido de carbono, así como los sensores fotoeléctricos, térmicos.

Detecte cualquier peligro en su empresa.

- Detección de humo
- Extinción a base de agua
- Extinción con agentes limpios
- Alarma de incendio y voceo digital
- Sensores de Flama o Gas
- Sensores de Monóxido de Carbono (CO2)
- Sensores Fotoeléctricos, Térmicos

### **Rastreo Vehicular**

Monitoreo de Alarmas

Este servicio nos permite localizar vehículos, personas u objetos por medio de un sistema satelital GPS.



### **CAMPANAS ELECTROMAGNETICAS**

Es un dispositivo capaz de producir una señal sonora al pulsa un interruptor. Su funcionamiento se basa en fenómenos electromagnéticos.

Consiste en un círculo eléctrico compuesto por un generador, un interruptor y un electroimán. La armadura del electroimán está unida a una pieza metálica llamada martillo, que puede golpear una campana pequeña.

### **Funcionamiento**

Al cerrar el pulsador, la corriente circula por el enrollamiento del electroimán y este crea un campo magnético en su núcleo y atrae la armadura. El martillo, soldado a la armadura, golpea la campana produciendo el sonido. Al abrir el interruptor cesan la corriente y el campo magnético del electroimán, y un resorte devuelve la armadura a su posición original para interrumpir el sonido.

Para conseguir que el martillo golpee la campana repetidamente mientras el interruptor esté cerrado, y no una sola vez, se sitúa un contacto eléctrico en la armadura que actúa como un interruptor. Así, cuando la armadura es atraída por el electroimán, se interrumpe el contacto, cesa la corriente en el electroimán y la armadura retrocede a su posición original. Allí vuelve a establecerse el contacto eléctrico, con lo que el electroimán vuelve a atraer a la armadura, y así sucesivamente.

Modernamente, muchos timbres no tienen interruptor, basándose en golpear la campana al doble de la frecuencia de la red. Tienen la ventaja de ser más fiables y más duraderos, ya que no se ensucian ni se desgastan los contactos del interruptor. Algunos no tienen ni campana, bastando la vibración de los contactos transmitida a la caja del timbre, A veces se llama zumbadores a estos timbres sin campana, porque el sonido que producen es un zumbido.

Normalmente este se usa en oficinas, escuelas e institutos para avisar que es la hora de cambiar de clase o si hay algún incendio.

Otra forma de explicar el funcionamiento es que al cerrar el interruptor, la corriente circula por el enrollamiento del electroimán y este crea un campo magnético en su núcleo y atrae la armadura.

El martillo, soldado a la armadura, golpea la campana produciendo el sonido. Al abrir el interruptor cesan la corriente y el campo magnético del electroimán, y un resorte devuelve la armadura a su posición original para interrumpir el sonido.

Para conseguir que el martillo golpee la campana repetidamente mientras el interruptor esté cerrado, y no una sola vez, se sitúa un contacto eléctrico en la armadura que actúa como un interruptor. Así, cuando la armadura es atraída por el electroimán, se interrumpe el contacto, cesa la corriente en el electroimán y la armadura retrocede a su posición original. Allí vuelve a

establecerse el contacto eléctrico, con lo que el electroimán vuelve a atraer a la armadura, y así sucesivamente.

## **CAMPANAS DE INDUCCIÓN ELECTROMAGNÉTICA**

Esta nueva tecnología en iluminación eficiente, utiliza elementos fluorescentes SIN ELECTRODOS, lo que hace que aumente considerablemente su vida útil en hasta 8 veces más que una lámpara de haluro metal y con un ahorro energético de al menos un 50%.

Para generar luminiscencia por Inducción Electromagnética, se necesitan 3 elementos básicos:

- Un generador que induce un campo electromagnético;
- Una antena que produce una ionización de gas de mercurio a baja presión;
- Un bulbo que contiene el elemento luminiscente.

Las Lámparas de Inducción Electromagnética son **AMPLIAMENTE VENTAJOSAS** en comparación a las lámparas de Haluro Metal y sus beneficios son indiscutibles..... **VENTAJAS DE LA INDUCCION ELECTROMAGNETICA vs. HALURO METAL.**

### **Inducción-Electromagnética-Interna=vs.=Externa**

Existen-2-tipos-de-lámparas-de-Inducción-Electromagnéticas:

Inducción-electromagnética-Interna o de Alta-Frecuencia-e;

Inducción-electromagnética-Externa o de Baja-Frecuencia.

Su denominación depende de la posición del elemento electromagnético que produce-la-inducción-en-relación-al-bulbo-fluorescente.

Inducción Electromagnética Interna: Se caracteriza porque el elemento que genera la inducción electromagnética (Antena) va instalado dentro del elemento-fluorescente-(bulbo).

Inducción Electromagnética Externa: La generación de la inducción electromagnética es efectuada por 2 anillos metálicos que van instalados por fuera del elemento fluorescente-(bulbo), abrazándolo-en-ambos-extremos.

Si bien es ciertos que ambas lámparas se basan en el mismo principio, sus diferencias tecnológicas son significativas.

## LED

Los LED son componentes eléctricos semiconductores (diodos) que son capaces de emitir luz al ser atravesados por una corriente pequeña. Las siglas "LED" provienen del inglés "Light Emitting Diode", que traducido al español es "Diodo Emisor de Luz". Dos materiales conductivos cualesquiera forman un diodo-cuando-son-puestos-en-contacto.

Su vida útil estimada de 40 a 50 mil horas los hace muy atractivos, ya que no requieren-mantenimiento-y-son-muy-amigables-con-el-medio-ambiente.

Por su muy bajo consumo, esta tecnología es también utilizada en Luminarias de Patios, Estacionamientos y Calles, alimentadas mediante energía de la red eléctrica normal o con energía solar mediante colectores fotovoltaicos y acumuladores. En este último caso, son especialmente sugeridas para ubicaciones físicas remotas, sin disponibilidad de una red de energía tradicional, que cuenten con una cantidad de horas-de-luz-diurna-adecuada.

Ventajas de los LED's:

Son muchas las ventajas que poseen los LEDs ante los dispositivos tradicionales de iluminación como bombillas incandescentes, halógenos, tubos de-neón, etc.

A continuación enumeramos algunas de ellas:

- Reducen significativamente el consumo energético en comparación a las luminarias tradicionales tales como las bombillas incandescentes, alógenos, entre otros.
- Tiempo estimado de vida muy elevado, por lo que se reducen costos de mantenimiento.
- Trabajan a muy baja corriente y tensión lo que los hace más seguros y confiables-en-su-implementación.
- Virtualmente no generan calor (cuando son implementados a baja potencia).
- Por ser de estado sólido pueden ser adaptados a aplicaciones con ciertos grados-de-vibraciones-o-impactos.

- Son excelentes para ser implementados en sistemas micro controlados o con niveles-de-tensión-TTL-por-trabajar-a-bajo-voltaje.
- Tiempo de respuesta ON/OFF - OFF/ON virtualmente instantáneo.
- Puede ajustarse su intensidad en el brillo por medio de modulación en frecuencia.
- Son ideales para el diseño de dispositivos de iluminación multicolor.
- Permiten la elaboración de dispositivos de iluminación mucho más prácticos y de fácil instalación.

### TUBOS FLUORESCENTES DE BAJO CONSUMO

Los Tubos T5 de bajo consumo reemplazan a los tradicionales tubos fluorescentes-de-40w-y-20w.

#### **BENEFICIOS:**

- Menor consumo (un 30% menos consumo)
- Mayor Luz (generan un 20% de más luz)
- Mayor Vida Útil (estimada en 8.000 horas, es decir 3 a 4 veces la de los tubos tradicionales)
- Menor costo de mantención, tanto en mano de obra como en suministros.
- Disipan menos calor y por lo tanto bajan los riesgos de sobrecalentamiento (incendio).
- Sin efecto Estroboscópico lo que disminuye el cansancio y stress.
- Menor contaminación (solo 1,3mg de Hg)

### **AMPOLLETAS COMPACTAS**

Rectas y Espirales.

Estas bombillas fluorescente compacta permiten reemplazar ampolletas incandescentes de 220V, desde 10 a 600 watts. No requieren balast ni partidador.

#### **BENEFICIOS:**

- Menor=consumo
- Larga-vida-útil:=8.000-horas.
- Bajo costo de mantención, tanto en mano de obra como en suministros.
- Sin efecto Estroboscópico lo que disminuye el cansancio y stress.
- Se instalan en los mismos portalámparas actuales (Roscas E40, E27 y otras)

- Pueden ser utilizadas en diferentes Proyectores, Campanas, Luminarias
- Menor contaminación (Amigable con el medio ambiente).

Información de Interés: FLUORESCENCIA vs. INCANDESCENCIA

Al iluminar Galpones, Áreas de carga, Áreas de trabajo, se recomiendan para alturas de hasta 3 a 4 metros.

TIMBRE DE CAMPANA ELECTROMAGNÉTICO T-15

Timbre de campana Ø15 cm.

NO produce interferencias.

Funcionamiento continuo SIN CALENTAMIENTO.

Variedad de TENSIONES.

APLICACIONES: Alarmas de incendios, escuelas, parkings, peajes, grandes superficies, almacenes y otros.

### **SIRENA ELECTRÓNICAS**

Sirenas electrónicas para alerta temprana y notificación de emergencias



Los dispositivos acústicos han sido utilizados para proporcionar alerta ante situaciones de emergencia durante siglos. En tiempos antiguos se alertaba al hacer chocar objetos metálicos entre sí, luego se construyeron campanarios, y ya en el siglo 20 comenzaron a aparecer las sirenas mecánicas rotativas, las que aún son usadas en muchos países. Sin embargo, el desarrollo electrónico también ha influido de gran manera esta industria, las primeras sirenas electrónicas empezaron a aparecer a finales del siglo 20. Las sirenas electrónicas básicamente son amplificadores electrónicos de alto desempeño,

parecidos a los instalados en sistemas domésticos de sonido. No obstante, estas sirenas trabajan con niveles de salida substancialmente mayores y consideran exigencias particulares relacionadas con alta fiabilidad y variación en sus métodos de control, requeridos en este tipo de sistemas. La infraestructura de control requiere ser altamente fiable y generalmente se disponen dos canales independientes de comunicación. Los parlantes para estos amplificadores son dispuestos en deflectores de sonido (bocinas) diseñados especialmente, los que emiten señales almacenadas en la memoria digital de la sirena o señales alimentadas desde fuentes – micrófono, teléfono, estación de radio, radio común, radiodifusión televisiva etc. – Telegrafía actualmente ofrece dos líneas de sirenas electrónicas: PAVIAN y GIBON. Un nuevo ítem incorporado es la sirena compacta integrada SCREAMER

#### Requisitos contemporáneos de las sirenas electrónicas

Tanto las aplicaciones como características técnicas de las sirenas son regidas por ley en muchos países desarrollados. A pesar que los requerimientos son prácticamente los mismos, desde un punto de vista técnico difieren tanto que no pueden ser satisfechos mediante una única versión de sirenas. Por esta razón, las sirenas desarrolladas por Telegrafía siguen una filosofía modular, con la que se pueden establecer sistemas que se adecúen a las condiciones particulares, en cuanto a sus requerimientos de señal acústica, control de la red de sirenas y revisión de su estado. Al momento de su diseño, además, se debe prestar gran atención a asegurar su funcionamiento incluso ante situaciones en las que su suministro energético principal falle, algo posible en situaciones de emergencia, por lo que estas cuentan con sistemas suplementarios de energía.

#### Principales ventajas de las sirenas electrónicas:

- Su operación estándar utiliza baterías que son recargan continuamente.
- Son capaces de reproducir tanto señales de alerta como anuncios por voz.
- Es posible conectarlas a fuentes externas de señal – micrófono, teléfono, radio estación, radio, etc.
- Incorporan avanzadas rutinas automáticas de auto-diagnóstico – las potenciales fallas son detectadas previo a su potencial uso, pudiendo ser corregidas a tiempo

#### Principales desventajas de las sirenas motorizadas:

- Tienen un excesivo consumo de energía y requieren un suministro continuo de energía eléctrica – su operación mediante baterías es

imposible o un sistema de respaldo energético sería excesivamente costoso.

- Solo son capaces de reproducir tonos de cierta frecuencia o tonos oscilantes; los anuncios por voz no son una opción.
- Su operación es manual.
- No poseen funciones de auto-diagnóstico.

#### Sirena electrónica PAVIAN

Audio sirena de alarma sistemas de alarma de seguridad sirena de alerta

Las sirenas electrónicas PAVIAN representan el mayor nivel de sistemas electrónicos ofrecidos por Telegrafía. Estos son dispositivos electrónicos modulares principalmente diseñados para establecer sistemas de alerta temprana de gran envergadura, los cuales requieren un sofisticado control y monitoreo del estado de sus componentes. También pueden funcionar como dispositivos controlados localmente cuando sea requerido, ya sea por razones de respaldo, interacción con el medio ambiente o reacción a señales externas. Estos equipos permiten una completa interacción externa, donde puede reaccionar en base a información recogida del medio ambiente o controlar otros dispositivos electrónicos.

Esta sirena electrónica es un sofisticado terminar acústico con una amplia variedad de métodos de control, y a la vez, incorpora interfaces y opciones de monitoreo y control sistemas ya implementados. Debido a los sistemas de monitoreo muchas veces es parte de un sistema de alerta, la implementación de las sirenas PAVIAN permiten reducir los costos globales del proyecto, con respecto a establecer estos sistemas separados. Es posible establecer distintos tipos de arreglos de figuras de distribución sonoras, con niveles de potencia entre 300 W y 4,500 W.

#### Sirena electrónica GIBON

Sirena electrónica alerta pública defensa civil

GIBON es una sirena electrónica entrega distribución sonora de alta calidad en las zonas amenazadas a un precio optimizado. Su diseño esta principalmente destinado a un equipo de alerta independiente, localmente controlado. Sin embargo, también puede ser utilizado para establecer sistemas simples de alerta. Es posible establecer distintos tipos de arreglos de figuras de distribución sonoras, con niveles de potencia entre 300 W y 1,200 W.

La sirena electrónica GIBON es generalmente controlada mediante botones situados directamente en la sirena, o a cierta distancia de estas. También es posible usar módulos de control locales más sofisticados y más capaces. Por otro lado, sistemas terceros de comunicación y control también pueden ser usados para controlar las sirenas GIBON.

#### Sirena electrónica integrada SCREAMER

Compacta sirena electrónica integrada dispositivo alerta emergencia Screamer  
sirena 12v sirena industrial

SCREAMER es una sirena electrónica integrada especializada en la distribución sonora, alerta temprana y sistemas de evacuación, este dispositivo es parte de la línea aSCADA. Su módulo electrónico es integrado directamente dentro de una bocina de aleación de aluminio de alta durabilidad, con un altavoz de gran poder presión acústica. Este módulo cuenta con un poderoso amplificador electrónico, memoria digital de señales de audio e interfaces de entrada para emitir los mensajes de alerta almacenados o voz en vivo.

El dispositivo SCREAMER está disponible en dos versiones: bocina corta o larga. La bocina corta tiene un patrón circular de distribución sonora, con menor presión acústica, mientras que la bocina larga genera un patrón elíptico de distribución sonora y mayor presión acústica. SCREAMER ofrece varias alternativas para asegurar la funcionalidad requerida – desde una simple configuración hasta la programación de los algoritmos necesarios. Es posible almacenar virtualmente un número ilimitado de reportes, definir sus prioridades, interrupciones y combinaciones, entre otros.

La sirena electrónica se compone de una unidad de control que ha almacenado en el interior de la secuencia de tonos, y uno o dos altavoces conectados a esta unidad. El uso de sirenas electrónicas está muy extendido, siendo especialmente adecuadas para su funcionamiento continuo, también tienen un bajo consumo eléctrico y no requieren mantenimiento

La sirena electrónica de última generación utiliza altavoces muy potentes (neodimio) que permiten una mayor audibilidad y, por tanto, una mayor eficacia. Algunos incluso han llegado a 200 voltios de potencia cada uno, y se pueden integrar en el techo del vehículo o en el motor.



## **BALIZAS**

Una baliza es un objeto señalizador, utilizado para indicar un lugar geográfico o una situación de peligro potencial. En topografía, el verbo balizar es usado para referirse a la acción de ubicar un sitio en relación a otros, fácilmente ubicables, que aseguran el poder encontrarlo posteriormente. En navegación, suele emplearse el término boya o boya de balizamiento.

Una baliza puede ser activa si emite una señal, sea del tipo que sea, o pasiva, si no emite.

Tipos de balizas activas:

Emisoras de señales de radio (satélites GPS).

Emisoras de señales luminosas (faro).

Emisoras de señales ultrasonido (sonar).

Las balizas definidas en las normas internacionales, en manera genérica son definidas como: balizas de baja intensidad, de media intensidad y de alta intensidad luminosa:

Balizas de baja intensidad, color rojo sirven para la señalización nocturna.

Balizas de media intensidad, color rojo sirven para la señalización nocturna.

Balizas de media intensidad, color blanco sirven para la señalización nocturna y diurna.

Balizas de alta intensidad, color blanco sirven para la señalización diurna y nocturna (con intensidad reducida).

Las balizas para la señalización de obstáculos fijos se colocan en todas las estructuras que pueden presentar un peligro para los aeromóviles y helicópteros, en las proximidades de los aeropuertos o helipuertos como

también en obstáculos que sobresalen en un zona de circulación de aviones y helicópteros, como antenas radio, edificios, chimeneas, líneas de alta tensión, o cualquier otro objeto con estructura abierta u opaca.

Una baliza es un objeto señalizador, utilizado para indicar un lugar geográfico o una situación de peligro potencial. En topografía, el verbo balizar es usado para referirse a la acción de ubicar un sitio en relación a otros, fácilmente ubicables, que aseguran el poder encontrarlo posteriormente. En navegación, suele emplearse el término boya o boya de balizamiento.

Una baliza puede ser activa si emite una señal, sea del tipo que sea, o pasiva, si no emite.

Tipos de balizas activas:

Emisoras de señales de radio (satélites GPS).

Emisoras de señales luminosas (faro).

Emisoras de señales ultrasonido (sonar).

### **Baliza Electrónica**

CIRCUITO QUE EMITE UNA BALIZA EN TELEGRAFIA CONFIGURABLE

ESTE CIRCUITO PERMITE EMITIR UNA BALIZA EN TELEGRAFIA

EL CUAL PODEMOS CONFIGURAR EL TIEMPO DE ESPERA DESDE QUE NO RECIBE NINGUNA SEÑAL Y TAMBIEN EL TIEMPO ENTRE BALIZAS

SI EN EL MOMENTO DE EMITIR LA BALIZA HAY ACTIVIDAD EN EL REPETIDOR ESTA ESPERARA A QUE FINALICE LA MISMA

PODEMOS CAMBIAR LA BALIZA, LA VELOCIDAD Y EL TONO DE LA MISMA A TRAVES DEL PUERTO SERIE DEL ORDENADOR SIN NECESIDAD DE TENER QUE DESMONTARLA

Tipos

Baliza Solar Para Torres Y Antenas

Marco Frente Adaptador Ford Ka Azul S/ Baliza 96´

Señalización Vial, Baliza, Ruta, Caminos. Leds Solar

Linterna Táctica Baliza 1200lm Zoom Cargador 220/12v Box Pvc

Secuenciador Intermitente Para Led's 2 Canales Tipo Baliza

Matafuegos Abc 5 Kg Baliza Y Soporte Habilitación

LCD.

A las matrices de 5x7 siguen las líneas de caracteres, principalmente LCD y VFD, presentándose en múltiples formatos, de una a cuatro líneas de ocho a cuarenta caracteres.

Matriz gráfica. Consiste en una matriz más grande, que puede representar tanto caracteres como gráficos. Se fabrican en LCD y VFD. Las matrices de LED están constituidas por un mosaico de visualizadores más pequeños (8x8, normalmente). Pueden ser multicolores (Rojo-Naranja-Verde o Rojo-Verde-Azul), encontrando su utilidad en vallas publicitarias, campos de fútbol, etc.  
Visualizador (Display) electromecánico

Artículo principal: Visualizador electromecánico

Los problemas de los primeros visualizadores para su uso a la intemperie: falta de luminosidad y fragilidad condujeron al desarrollo de otros tipos de visualizador, en los que se mueve mecánicamente alguna pieza que oculta o muestra un símbolo o leyenda. Pertenecen a este tipo los visualizadores "de cortinilla", que constan de un motor paso a paso que va pasando las "hojas" que contienen distintas leyendas hasta llegar al mensaje deseado. Gozó de gran popularidad en aeropuertos, estaciones de tren y autobuses, etc. Pero la dificultad para cambiar los mensajes significó su fin cuando se pudo disponer de alternativas en otras tecnologías. Otro visualizador mecánico, que se ve como 7 segmentos y como matriz consiste en segmentos o puntos fluorescentes sobre láminas que pueden girar para ponerse perpendiculares mediante la acción de un electroimán. Presenta la ventaja de que son visibles a plena luz solar y sólo consumen en el cambio de estado.

Visualizador de proyección

Artículo principal: Visualizador de proyección

Despiece de un visualizador de proyección. Se pueden apreciar las bombillas, grupos de lentes, película conteniendo los dígitos y diafragmas. Consisten en una matriz de lámparas, de las que se ilumina sólo una cada vez. La luz se dirige a un condensador que la proyecta sobre una película que contiene los símbolos que se quiere representar. Después otro grupo de lentes enfoca la imagen sobre una pantalla translúcida, que se hacen visibles en su cara posterior. Como norma general el número de imágenes está limitado a doce y no se pueden cambiar, salvo que se desmonte la unidad y se cambie la película.

El displays de 7 segmentos, es un componente que se utiliza para la representación de números en muchos dispositivos electrónicos.

Cada vez es más frecuente encontrar LCD's en estos equipos (debido a su bajísima demanda de energía), todavía hay muchos que utilizan el display de 7 segmentos por su simplicidad.

Este elemento se ensambla o arma de manera que se pueda activar cada segmento (diodo LED) por separado logrando de esta manera combinar los elementos y representar todos los números en el display (del 0 al 9).

El display de 7 segmentos más común es el de color rojo, por su facilidad de visualización.

Cada elemento del display tiene asignado una letra que identifica su posición en el arreglo del display. Ver el gráfico arriba

- Si se activan todos los segmentos se forma el número "8"
- Si se activan solo los segmentos: "a, b, c, d, f," se forma el número "0"
- Si se activan solo los segmentos: "a, b, g, e, d," se forma el número "2"
- Si se activan solo los segmentos: "b, c, f, g," se forma el número "4"

## **Pulsadores, alámbricos e inalámbricos**

### **PULSADOR**

Un botón o pulsador es un dispositivo utilizado para realizar cierta función. Los botones son de diversas formas y tamaño y se encuentran en todo tipo de dispositivos, aunque principalmente en aparatos eléctricos y electrónicos.

#### **Pulsador Alámbrico**

Los botones son por lo general activados, al ser pulsados con un dedo. Permiten el flujo de corriente mientras son accionados. Cuando ya no se presiona sobre él vuelve a su posición de reposo.

Puede ser un contacto normalmente abierto en reposo NA o NO (Normally Open en Inglés), o con un contacto normalmente cerrado en reposo NC.

Descripción

Consta del botón pulsador; una lámina conductora que establece contacto con los dos terminales al oprimir el botón, y un muelle que hace recobrar a la lámina su posición primitiva al cesar la presión sobre el botón pulsador.

## Tipos

Diferentes tipos de pulsadores: (a) Basculante. (b) Pulsador timbre. (c) Con señalizador. (d) Circular. (e) Extraplano.

## Funcionamiento

El botón de un dispositivo electrónico funciona por lo general como un interruptor eléctrico, es decir en su interior tiene dos contactos, al ser pulsado uno, se activará la función inversa de la que en ese momento este realizando, si es un dispositivo NA (normalmente abierto) será cerrado, si es un dispositivo NC (normalmente cerrado) será abierto

## PULSADORES DE ALARMA Y DE EXTINCIÓN ¿SABES DIFERENCIARLOS Y CONOCES SU ACTUACIÓN?

Quizás este post pueda parecer insulso por la simplicidad del tema, sin embargo, en nuestras visitas a instalaciones hemos detectado que hay un alto desconocimiento sobre “qué son” y sobretodo, “qué activan” los diferentes pulsadores instalados en las instalaciones. Piensa en tu instalación, ¿sabrías diferenciar y decir que actuación tienen los pulsadores de tu planta?

Debido a la confusión existente con los diferentes pulsadores utilizados en las instalaciones PCI y a la importancia de conocer su actuación, en este post vamos a hacer hincapié en la manera de diferenciar los pulsadores. Básicamente existen cuatro tipos de pulsadores:

- Pulsadores de alarma: Al pulsarlo, se activan los sistemas de comunicación de la situación de emergencia (alarmas ópticas, acústicas, megafonía,...). Estos pulsadores deben estar señalizados y ser de color rojo para cumplir las normas UNE 23008 y EN 54-11, según indica el Reglamento de Instalaciones de Protección contra Incendios (<http://goo.gl/2kzPf>).
- Pulsadores de disparo de extinción: Al pulsarlos, se pone en marcha el sistema fijo de extinción al que están asociados (agua, espuma, gas...). Estos pulsadores deben ser de color amarillo para cumplirla norma EN 54-11 (EN-12094-3).
- Pulsadores de paro de extinción: Lógicamente, son para realizar la parada del sistema de extinción activado por el pulsador amarillo. Estos pulsadores deben ser de color azul para cumplir con la norma EN 54-11 (EN-12094-3).

- Pulsadores de evacuación: Al pulsarlos, se realizan acciones asociadas a la evacuación (apertura puertas evacuación, sistema de megafonía,...). Estos pulsadores deben ser de color verde para cumplirla norma EN 54-11

La realidad es que esta normativa es desconocida, los trabajadores no saben el código de colores, y además, no saben que función tiene cada uno de los pulsadores instalados en su instalación. Aún es más preocupante que algunos fabricantes no utilicen el código de colores ya que, suponemos, conocen la normativa. Este hecho da lugar a que en las instalaciones haya pulsadores de cualquier color para la alarma y/o la extinción.

Por ello, una buena práctica utilizada en algunos lugares es etiquetar los pulsadores indicando cuál es la función que realizan. De esta manera, todos sabrán utilizarlos y la respuesta ante una emergencia será la más efectiva posible.

### **Pulsadores Inalámbricos**

El transmisor portátil es el famoso PULSADOR INALÁMBRICO, el cual funciona con pilas. Al presionar el botón por un mínimo de 2 segundos, enviará una señal codificada digitalmente al receptor (cuenta con más de un millón de códigos posibles).

Cuando el receptor en su memoria (OJO, esto es clave), se activa el replay de salida, el cual tiene cuatro configuraciones opcionales: enganchado por 1 segundo, 4 segundos, hasta que sea reseteado o del tipo on/off. Hasta 32 trasmisores pueden ser programados en la memoria de este receptor.

En caso de robo con intimidación (asaltos), el sistema puede contar con pulsadores inalámbricos que se activan a distancia y envían una señal silenciosa a la central de monitoreo. Estos pulsadores pueden ser tan pequeños como un llavero

### **TRANSMISOR INALAMBRICO INTERLOGIX BLANCO**

Descripción - Arrow Prev - Arrow Next

Modelo: 60-670-95R

El Transmisor inalámbrico 60-688-95 fue creado para satisfacer la demanda de sensores de seguridad menos visibles para la detección de intrusiones residenciales y comerciales.

Código Fábrica: 4202.50.78.35 Marca: Interlogix

### **PULSADOR INALAMBRICO 4 BOTONES INTERLOGIX**

## Descripción-Arrow Prev-Arrow Next

Modelo: 600-1064-95R

El pulsado inalámbrico 600-1064-95r es un micro Mando pequeño y potente de pantalla táctil que funciona como una llave electrónica para armar y desarmar los sistemas de forma inalámbrica. La funcionalidad incluye la capacidad de activar la policía o alarmas de pánico auxiliares, encender o apagar las luces, abrir una puerta de garaje, todo ello desde hasta 500 metros de distancia.

### **Pulsadores de asalto (Botón de Pánico)**



Son solo pulsadores de alarma de contactos secos que permitirá activar el sistema sin que suene la sirena en caso de asalto. Se podrán instalar en los baños, bajo mesas, etc.

También lo hay como receptor con llavero inalámbrico, puede ser utilizado como botón de pánico o activar desactivar la alarma.



Receptora inalámbrica para Botones de pánico o accesorios inalámbricos.

### **g. Elección de tecnología para el diseño óptimo de sistemas de seguridad**

Todo proyecto permite una organización general de la idea de protección y reducción de riesgos que todo diseñador o instalador de seguridad debe realizar para concretar una actividad PROFESIONAL de relevancia.

Se deberá tener en cuenta para el diseño óptimo de sistema de seguridad lo siguiente:

- a) El tipo de inmueble
- b) La zona donde se encuentra emplazado el mismo
- c) Los requerimientos del usuario
- d) Los riesgos a los que puede estar sometido el inmueble
- e) El tiempo de ejecución de la obra.
- f) Los insumos, equipos y dispositivos a adquirir e instalar.
- g) Las facilidades de conexión de todos y cada uno de los elementos intervinientes.
- h) Los costos de mano de obra, equipos y proyectistas, a fin de presupuestar económicamente a un precio justo y beneficioso para ambas partes.
- i) Los tiempos de ejecución, proyecto y puesta en marcha.

Los sistemas electrónicos de seguridad se pueden clasificar de la siguiente manera, los que nos servirán para la elección tecnológica del sistema de seguridad óptimo que se desea implementar estilos son:

- Sistemas contra robo/asalto
- Circuitos Cerrados de Televisión (CCTV)
- Sistemas de control de los accesos
- Sistemas de aviso de incendio

#### **Sistemas contra asaltos y robos**

Estos sistemas presentan los siguientes bloques operativos de relevancia:

- a) Central de gobierno o Panel de Control
- b) Subsistema de DETECCIÓN

- c) Subsistema de SEÑALIZACIÓN
- d) Activación y/o programación general
- e) Alimentación o energía del sistema

Se deberá en lo posible seguir estos pasos o secuencia:

1. Analizar las características del ocal y de la actividad que se realiza en ella además del tipo de materiales que existe para determinar el grado de seguridad que le corresponde, al respecto existen normas técnicas que definen estos grados quedando establecido que existen cuatro grados de seguridad en función del riesgo, quedando en esta Orden asignados, además, en virtud de la naturaleza y características del lugar en el que se va a efectuar la instalación y de la obligación, o no, de estar conectados a una central de alarmas o centro de control, del modo siguiente:
  - a) Grado 1, o de bajo riesgo, para sistemas de alarma dotados de señalización acústica, que no se vayan a conectar a una central de alarmas o a un centro de control.
  - b) Grado 2, de riesgo bajo a medio, dedicado a viviendas y pequeños establecimientos, comercios e industrias en general, que pretendan conectarse a una central de alarmas o, en su caso, a un centro de control
  - c) Grado 3, de riesgo medio/alto, destinado a establecimiento obligados a disponer de medidas de seguridad, así como otras instalaciones comerciales o industriales a las que por su actividad u otras circunstancias se les exija disponer de conexión a central de alarmas o, en su caso, a un centro de control.
  - d) Grado 4, considerado de alto riesgo, reservado a las denominadas infraestructuras críticas, instalaciones militares, establecimientos que almacenen material explosivo reglamentado, y empresas de seguridad de depósito de efectivo, valores, metales preciosos, materias peligrosas o explosivos, requeridas, o no, de conexión con central de alarmas o, en su caso, a centro de control.
2. El sistema de seguridad debe, en lo posible, estar conectado a una Central de Alarmas (CRA) homologada. Esto garantiza la atención a su alarma 24 horas, 365 días al año. Solicite información sobre el canal de conexión del sistema de alarma con la CRA, y sobre sistemas de comunicación como GPRS para asegurarse la comunicación en todo momento.
3. El sistema a instalar debe contar con un protocolo de seguridad cuando salta la alarma, a quien llaman cuando salta la alarma, si llaman al local, cómo se notifican las incidencias, cómo se cambia la palabra clave, quien

llama a la Policía, etc. Un servicio de ayuda inmediata puede facilitar la atención a incidencias.

4. El usuario debe tener un acceso inmediato al sistema: solicite que su alarma pueda ser gestionada desde su Smartphone (Tablet, portátil o PC), y que usted pueda verificar vía imágenes lo que sucede en su local.
5. Códigos de acceso: el sistema de seguridad debería permitir la creación de distintos códigos de acceso para sus empleados y para el usuario, y que estos puedan ser actualizados con rapidez.
6. Otro factor importante para la elección es el presupuesto disponible para la implementación del mejor sistema de seguridad.

## **h. El Circuito Cerrado de Televisión (CCTV)**

Circuito cerrado de televisión o CCTV (siglas en inglés de closed circuit televisión) es una tecnología de videovigilancia diseñada para supervisar una diversidad de ambientes y actividades.

Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión, todos sus componentes están enlazados. Además, a diferencia de la televisión convencional, este es un sistema pesando para un número limitado de espectadores y para Emisoras de Radio AM.

El circuito puede estar compuesto, simplemente, por una o más cámaras de vigilancia conectadas a uno o más monitores de vídeo o televisores, que reproducen las imágenes capturadas por las cámaras. Aunque, para mejorar el sistema, se suelen conectar directamente o enlazar por red otros componentes como vídeos o computadoras.

Se encuentran fijas en un lugar determinado. En un sistema moderno las cámaras que se utilizan pueden estar controladas remotamente desde una sala de control, donde se puede configurar su panorámica, enfoque, inclinación y zoom. A este tipo de cámaras se les llama PTZ (siglas en inglés de pan – tilt – zoom)

Estos sistemas incluyen visión nocturna, operaciones asistidas por ordenador y detección de movimiento, que facilita al sistema ponerse en estado de alerta cuando algo se mueve delante de las cámaras. La claridad de las imágenes puede ser excelente, se puede transformar de niveles oscuros a claros. Todas estas cualidades hacen que el uso del CCTV haya crecido extraordinariamente en estos últimos años.

Es posible armar un círculo cerrado de televisión con una o más cámaras filmadoras conectadas a uno o más televisores o monitores, que se encargan de reproducir las imágenes. Si se agrega una grabadora, los vídeos pueden ser almacenados.

Los círculos cerrados de televisión son frecuentes en las empresas. Muchas optan por instalar cámaras en la entrada, la recepción, las oficinas, la fábrica y el depósito, con los monitores situados en un salón especial a cargo de una persona de vigilancia, quien deberá intervenir o dar aviso a la policía en el caso de detectar algún movimiento extraño.

Dependiendo de la tecnología y de la marca, entre otros factores, las cámaras utilizadas para configurar un círculo cerrado tienen precios muy alternativas. Los equipos más económicos suelen ofrecer imágenes cada cierto segundo, en lugar de una secuencia de vídeo ininterrumpida, aunque esto no siempre depende de la cámara utilizada.

Cuando la monitorización es remota, o sea que una o más personas asumen las tareas de observar todos los movimientos de un domicilio desde otro punto geográfico, la fluidez de las imágenes responde en parte a la velocidad de conexión a internet disponible en el puesto que desee vigilarse. Por otro lado, cabe mencionar que incluso en los casos en los que se envían vídeos normales existe un cierto retraso, ya que la información debe viajar de un sitio a otro.

## **EL CCTV**

Estos sistemas son una de los eslabones importantes de la cadena de seguridad electrónica integral de inmuebles pues permiten la observación a distancia de distintos eventos que pueden ser considerados como indeseables. Además es una importante herramienta de DISUACIÓN para el eventual ladrón pues lo intimida dejando de lado su interés de intentar un asalto o robo, además de ser una buena prueba ante la justicia local.

Consisten en CÁMARAS, Y LENTES los que ubicados estratégicamente y conectado a través de líneas de transmisión (coaxial multifilar o fibra óptica) a los monitores de TV permiten la visualización a distancia y controlar sectores estratégicos del inmueble. Pueden ser cableados o inalámbricos lográndose vía Radio Frecuencia la comunicación entre cámara y monitor. Equipos adicionales como secuenciadores y multiplexores, permiten la conexión de varias cámaras en un mismo monitor para observar, secuencialmente o en forma particionada más de una imagen en forma simultánea. La grabación de las imágenes con VCR es de suma importancia en instancias judiciales.

El circuito cerrado de televisión es el sistema más usado por las instituciones, locales industriales, locales comerciales, etc., para vigilancia de sectores específicos de dichos locales, especialmente en las entradas y en las zonas donde existen movimientos logísticos.

### **CCTV en vídeo vigilancia**

En esta aplicación el circuito estará compuesto, aparte de las cámaras y monitores, de un dispositivo de almacenamiento de vídeo (DVR Digital Vídeo Recorder, NVR Network Vídeo Recorder) dependiendo la estructura del circuito ya sea analógico o basado en redes IP, aunque se pueden realizar combinaciones dependiendo las necesidades del sitio. Las cámaras pueden ser fijas, con zoom, móviles o PT (pan. Tilt) o PTZ (Pan, Tilt, Zoom) como por ejemplo debido a la forma de domo invertido que presentan, y las cámaras con posicionador, que pueden ser remotamente movibles. Este movimiento se puede hacer mediante una consola o teclado mediante el cual se pueden manejar las diversas opciones del software instalado en ésta. Constan también en un sistema CCTV de videovigilancia dispositivos como: lámparas infrarrojas, sensores crepusculares, posicionadores, teleobjetivos, análisis de video y video inteligente, etc. La tecnología de las cámaras permiten actualmente según los modelos, captar imágenes térmicas en total oscuridad, o imágenes en oscuridad iluminadas con infrarrojos que la vista no es capaz de ver.

### **Diferentes funciones del CCTV**

- Visión en directo y grabación de imágenes: Permite tener pruebas visuales al producirse una incidencia.
- Gestión personal directa: Usted mismo podrá controlar diferentes zonas con una consola de fácil manejo
- Control desde Internet: Supervisión del recinto protegido desde cualquier lugar con conexión a Internet.
- Verificación visual de alarmas: Al detectarse una incidencia, se puede comprobar la naturaleza del suceso desde la CRA y ofrecer una respuesta más efectiva.
- Realización de tele – rondas o tele vigilancia: Desde la CRA se establecerá un contacto visual periódico con el recinto protegido para comprobar el estado de normalidad.

Vea lo que quiera, cuando quiera y desde donde quiera.

Sólo se necesita un ordenador conectado a Internet y, con un software de fácil manejo, se puede gestionar el sistema de CCTV sin que deje de grabar las imágenes en ningún momento. De esta forma podrá controlar sus instalaciones a distancia.

## **SISTEMAS DE POSICIONAMIENTO SATELITAL**

El Sistema de Posicionamiento Global (GPS) es un sistema de radionavegación de los Estados Unidos de América, basado en el espacio, que proporciona servicios fiables de posicionamiento, navegación, y cronometría gratuita e ininterrumpidamente a usuarios civiles en todo el mundo. A todo el que cuente con un receptor del GPS, el sistema le proporcionará su localización y la hora exacta en cualesquiera condiciones atmosféricas, de día o de noche, en cualquier lugar del mundo y sin límite al número de usuarios simultáneos.

El GPS se compone de tres elementos: los satélites en órbita alrededor de la Tierra, las estaciones terrestres de seguimiento y control, y los receptores del GPS propiedad de los usuarios. Desde el espacio, los satélites del GPS transmiten señales que reciben e identifican los receptores del GPS; ellos, a su vez, proporcionan por separado sus coordenadas tridimensionales de latitud, longitud y altitud, así como la hora local precisa.

Hoy están al alcance de todos en el mercado los pequeños receptores del GPS portátiles. Con esos receptores, el usuario puede determinar con exactitud su ubicación y desplazarse fácilmente al lugar a donde desea trasladarse, ya sea andando, conduciendo, volando o navegando. El GPS es indispensable en todos los sistemas de transporte del mundo ya que sirve de apoyo a la navegación aérea, terrestre y marítima. Los servicios de emergencia y socorro en casos de desastre dependen del GPS para la localización y coordinación horaria de misiones para salvar vidas. Actividades cotidianas como operaciones bancarias, de telefonía móvil e incluso de las redes de distribución eléctrica, ganan en eficiencia gracias a de la exactitud cronométrica que proporciona el GPS. Agricultores, topógrafos, geólogos e innumerables usuarios trabajan de forma más eficiente, segura, económica y precisa gracias a las señales accesibles y gratuitas del GPS.

Los sistemas de posicionamiento satelital son sistema que utilizan las señales de rebote de los satélites que circundan la tierra para determinar el lugar más o menos exacto en que se encuentra el aparato de GPS. Este sistema es muy usado por las fuerzas armadas PNP, y compañías de seguro para ubicar determinado objeto importante.

GPS es un sistema de posicionamiento basado en la medición de la distancia a un mínimo de cuatro satélites simultáneos, que además, transmiten sus posiciones estimadas. Es posible determinar (en cualquier momento y bajo cualquier condición atmosférica), una posición precisa en cualquier punto de la superficie terrestre.

El sistema GPS comprende tres segmentos diferentes:

- El segmento espacial
- El segmento de control
- El segmento de usuarios

### **El Segmento Espacial**

Consiste de 24 satélites distribuidos en seis planos orbitales inclinados  $55^\circ$  respecto al ecuador y distribuidos en forma equidistante. Los satélites se mueven a una altura aproximada de 20600 km, completando dos revoluciones por día sidéreo. El segmento espacial está diseñado de tal forma que se pueda contar con un mínimo de 4 satélites visibles por encima de un ángulo de elevación de  $15^\circ$  en cualquier punto de la superficie terrestre, durante las 24 horas del día.

Cada satélite GPS lleva a bordo varios relojes atómicos muy precisos. Estos relojes operan en una frecuencia de fundamental de 10.23 MHz, la cual se emplea para generar las señales transmitidas por el satélite.

### **El segmento de Control**

El segmento de control estaba compuesto en sus orígenes por una estación de control maestro en Colorado – Spring (EEUU), 5 estaciones de observación y 4 antenas de tierra distribuidas entre 5 puntos muy cercanos al ecuador terrestre.

En la actualidad se han anexado varias estaciones de rastreo: Australia, Quito, Usno, Buenos Aires, Bahrain, Inglaterra.

El segmento de control tiene la función de:

- Supervisar y controlar continuamente el sistema satelital
- Determinar el tiempo del sistema GPS.
- Predecir las efemérides satelitales y el comportamiento de los osciladores en los satélites.
- Actualizar periódicamente la información de navegación para cada satélite en particular.

## El segmento del Usuario

El segmento de Usuario comprende a cualquiera que reciba las señales GPS con un receptor, determinando su posición y/o la hora. Algunas aplicaciones típicas dentro del segmento usuario son: la navegación en tierra, ubicación de vehículos, topografía, navegación marítima y aérea, control de maquinaria, etc.

### La señal GPS

Los satélites transmiten constantemente en dos ondas portadoras que viajan a la velocidad de la luz. Dichas ondas portadoras se derivan de la frecuencia fundamental (10.23MHz), generada por un reloj atómico muy preciso.

La portadora L1  $\Rightarrow$  frecuencia de 1575.42 MHz y longitud de onda de 19.05cm.

La portadora L2  $\Rightarrow$  frecuencia de 1227.60 MHz y longitud de onda de 24.45 cm.

Las ondas portadoras están diseñadas para llevar los códigos binarios C/A y P en un proceso conocido como modulación. Modulación significa que los códigos están superpuestos sobre la onda portadora.

### La señal GPS

Cada satélite transmite señales en ambas frecuencias, siendo éstas, las señales de navegación (códigos), y los datos de navegación y sistema (mensaje). Los códigos que se modulan en la señal son:

- El código C/A modula a una frecuencia de 1.023Mz (10.23/10). La secuencia total es de un milisegundo y la duración mínima de uno de sus estados es de 300 m. El código C/A se transmite actualmente sólo por medio de la frecuencia portadora L1.
- El código P o código de precisión modula a una frecuencia de 10.23MHz, La secuencia de este código es de 267 días y la duración mínima de uno de sus estados es de 29.31m. Se les ha asignado a las distintas satélites porciones de siete días.

## El Mensaje de Navegación

El conjunto completo de datos está subdividido en cinco subconjuntos de seis segundos de duración cada uno, lo que hace que el conjunto completo tiene un ciclo de tiempo de 30 segundos. En ellos podemos encontrar:

- ✓ Subconjunto 1: Datos de los parámetros de los relojes de los satélites.
- ✓ Subconjunto 2 y 3: Datos de las efemérides transmitidas

- ✓ Subconjunto 4 y 5: Datos del almanaque y parámetros ionosféricos.

Los subconjuntos 4 y 5 no se repiten cada 30 segundos. Ambos subconjuntos contienen 25 páginas que aparecen sucesivamente, Cada página contiene los datos de almanaque de un satélite, de tal modo que se dispone del contenido total de información cada 12.5 minutos.

### Principios de Posicionamiento

El principio del posicionamiento satelitario es simple y se basa en relacionar tras componentes:

- Una cantidad conocida, que es la posición del satélite ( $X^S, Y^S, Z^S$ ).
- Una cantidad mensurable, que es la distancia satélite receptor.
- Una cantidad desconocida, que es la posición del receptor ( $X_R, Y_R, Z_R$ )

La distancia satélite – receptor puede ser determinada por el receptor GPS. A partir de la distancia hacia un satélite y la posición de éste, sabemos que la posición del receptor debe ser en algún punto sobre la superficie de una esfera imaginaria cuyo origen es el satélite mismo. Si consideramos tres satélites y sus respectivas distancias al receptor podemos intersectar tres esferas imaginarias, con lo cual quedan definidos dos puntos de intersección. Uno de ellos será una posición ilógica para ser la de nuestro receptor y la podremos descartar.

### Medición de distancia satélite – receptor

Esta distancia se mide a partir del tiempo de propagación de la señal emitida desde el satélite. Los satélites y los receptores cuentan con relojes que controlan el tiempo de emisión y recepción de la señal respectivamente. De esta manera, la simple diferencia entre el instante de recepción y el de emisión proporciona el tiempo de propagación. Multiplicado por la velocidad de propagación de la señal dicho tiempo se convierte luego en la distancia satélite – receptor.

En los satélites se encuentran relojes atómicos que son controlados por la Estación de control.

Los satélites transmiten al usuario junto con la información orbital, las correcciones que deben ser aplicadas a sus relojes. No es posible equipar a los receptores con relojes de tan alta tecnología.

Por esta razón los relojes de los receptores pueden estar afectados de errores intolerables.

Debido a ello la distancia determinada satélite – receptor se denomina pseudodistancia.

Posición de los satélites ( $X^S, Y^S, Z^S$ )  $\Rightarrow$  dato conocido.

Pseudodistancia  $\Rightarrow$  la mide el receptor.

4 incógnitas  $\Rightarrow (X_R, Y_R, Z_R)$  y la corrección al reloj del receptor.

$\Rightarrow$  Se necesitan 4 pseudodistancias (4 satélites) para resolver el problema.

Para realizar la medición del tiempo de propagación de la señal usando código:

- 1) El receptor genera un código idéntico al del satélite
- 2) Mide el tiempo de desfase entre el código recibido y el replicado.

Efemérides del Sistema

Tres sistemas de datos están disponibles para la determinación de los vectores de posición y velocidad de los satélites en un marco terrestre de referencia para cualquier instante. Estos sistemas son:

#### DATOS DE ALMANAQUE

Provee al usuario d datos menos exactos para facilitar la búsqueda de los satélites por parte del receptor o para las tareas de planificación.

#### EFEMERIDES TRANSMITIDAS

Las estaciones de rastreo reciben las señales emitidas por los satélites (en un lapso de 7 días) y envían las observaciones a la Estación de Control Maestro, quien se encarga de calcular las órbitas de los satélites. A partir de éstas predice órbitas que describen el movimiento de los satélites en el futuro. Luego estas órbitas predichas son enviadas desde tierra a los satélites.

#### EFERMERIDES PRECISAS

Las efemérides precisas son determinadas por el international GPS Service (IGS), en base a los datos recogidos por sus estaciones de referencia GPS distribuidas por todo el globo terrestre. Son calculadas y no predichas, por lo cual no están disponible en tiempo real para los usuarios. Su precisión es del orden de 5 cm.

## **i. El control de alarmas. Los sistemas de control de alarmas, procedimientos de reacción ante alarmas**

### **EL CONTROL DE ALARMAS**

#### **Monitoreo de Alarmas**

Monitoreo de alarmas con sistemas digitales de diversas marcas que se adaptan a cualquier necesidad de oficinas, bodegas, industrias o comercios y que tienen una funcionalidad de 24 hrs los 365 días del año-

Es el servicio por el cual su Sistema de Alarma queda conectado a un panel de control que funciona como el cerebro del Sistema de Alarma misma que manda la señal a nuestra Estación Central que atiende y procesa las señales de emergencia.

La función de una alarma es “anunciar” la intrusión o intento de intrusión por alguna de las primeras barreras, actuando como escudo.

La mejor alarma es la que protege dos importantes zonas en su propiedad: La perimetral (exterior) y la del interior de la misma. Por eso es importante que cada puerta y ventana del inmueble se encuentren protegida con algún tipo de dispositivo.

El interior de su propiedad se protege utilizando sensores de movimiento. Los más comunes detectan la presencia de alguna persona, comparando la temperatura del cuerpo como la temperatura ambiente de una habitación.

### **SISTEMAS DE CONTROL DE ALARMAS**

#### **Conceptos básicos**

**Seguridad Física:** es el conjunto de recursos humanos, tecnológicos y operacionales, que tienen como propósito resguardar la vida, bienes, operación e información de las organizaciones, contra eventos o actos negativos no deseados.

#### **Seguridad Electrónica**

Es la parte de la seguridad física conformada por un conjunto de dispositivos electrónicos instalados estratégicamente y diseñados para el registro de diferentes tipos de eventos, detectar cambios de variables físicas como son: movimiento, sonidos, gases o humos, calor, infrarrojos etc. La información

capturada es almacenada y analizada, para la toma de acciones que mitiguen o combatan las acciones de riesgo detectados.

### **Sistema de alarmas**

Un sistema de alarma es un elemento de seguridad pasiva. Esto significa que no evitan una situación anormal, pero sí son capaces de advertir de ella, cumpliendo así, una función disuasoria frente a posibles problemas. Por ejemplo: La intrusión de personas. Inicio de fuego. El desbordamiento de un tanque. La presencia de agentes tóxicos. Cualquier situación que sea anormal para el usuario.

Son capaces además de reducir el tiempo de ejecución de las acciones a tomar en función del problema presentado, reduciendo así las pérdidas.

### **Funcionamiento**

Una vez que la alarma comienza a funcionar, dependiendo del sistema instalado, este puede tomar acciones en forma automática. Por ejemplo: Si se detecta la intrusión de una persona a un área determinada, mandar un mensaje telefónico a uno o varios números. Si se detecta la presencia de humo, calor o ambos, mandar un mensaje telefónico a uno o varios números o accionar la apertura de rociadores en el techo, para que apaguen el fuego. Si se detecta la presencia de agentes tóxicos en un área, cerrar las puertas para que no se expanda el problema.

Para esto, la alarma tiene que tener conexiones de entrada, para los distintos tipos de detectores, y conexiones de salida, para activar otros dispositivos que son los que se ocupan de hacer sonar la sirena, abrir los rociadores o cerrar las puertas.

Todos los sistemas de alarmas traen conexiones de entrada para los detectores y por lo menos una de salida para la sirena. Si no hay más conexiones de salida, la operación de llamar a un número, abrir el rociador o cerrar las puertas deberá ser realizada en forma manual por un operador.

Uno de los usos más difundidos de un sistema de alarma es advertir el allanamiento en una vivienda o inmueble. Los equipos de alarma pueden estar conectados con una Central Receptora, también llamada Central de Monitoreo, con el propietario mismo (a través de teléfono o TCP/IP) o bien simplemente cumplir la función disuasoria, activando una sirena que funciona a unos 90 db (la potencia de la sirena estará regulada por las distintas leyes de seguridad del Estado o región correspondiente).

Para la comunicación con una Central Receptora de Alarmas, se necesita de un medio de comunicación, como pueden serlo: una línea telefónica RTB o una línea GSM, un transmisor por radiofrecuencia llamado Trunking o mediante transmisión TCP/IP que utiliza una conexión de banda ancha ADSL y últimamente servicios de Internet por cable, Cable Módem.

Los sensores de movimiento son aparatos basados en la tecnología de los rayos infrarrojos o las ondas ultrasónicas para poder "mapear" o captar en tiempo real los movimientos que se generan en un espacio determinado. Estos sensores de movimiento, adscritos sobre todo a cámaras de seguridad, puertas en almacenes y centros comerciales, etc.; son uno de los dispositivos más reconocidos e importantes dentro de la seguridad electrónica, que tanto ha apostado por, sobre todo, dos aspectos fundamentales: el tamaño y la funcionalidad de cada uno de los equipos que usan durante el proceso. Y es que los sensores de movimiento que podemos ver, por ejemplo, encima de las entradas y salidas de establecimientos públicos que se activan con sólo la movilidad específica de los sujetos, cumplen a cabalidad con estas leyes, si se puede decir así, de la seguridad virtual que cada día, y como lo denotan varios artículos en este blog, nos sorprende cada día más.



### **Partes de un sistema de Alarma**

En el momento en el mercado encontramos una amplia gama de sistemas para detección de intrusión que van desde los Paneles de 4 zonas, hasta los modelos expandibles de hasta 128 zonas, sistemas totalmente integrados y adaptación de paneles para detección temprana incendios y control de accesos.

El usuario puede programar y solucionar problemas a distancia en los sistemas para intrusión de sistemas electrónicos mediante una PC.

Estos también ofrecen sistemas alámbricos, inalámbricos y combinados, monitorearles para uso comercial y domiciliario, además de una gama de opciones de comunicación alternativas entre las cuales se incluyen radio celular y de largo alcance.



### **Central de Alarma.**

La central de alarma es el cerebro de todo el sistema, posee un microprocesador que es encargado, de acuerdo a su programación, de recibir las señales de los sensores y tomar acciones como activar una sirena, un emisor telefónico, etc. La central dispone de un cargador automático para batería que será la encargada de alimentar a todo el sistema en caso de corte del suministro eléctrico.

### **Central procesadora.**

Es la CPU del sistema. En ella se albergan la placa base, la fuente y la memoria central.

Esta parte del sistema es la que recibe las diferentes señales que los diferentes sensores pueden emitir, y actúa en consecuencia, disparando la alarma, comunicándose con la central por medio de un modem, etc. Se alimenta a través de corriente alterna y de una batería respaldatoria, que en caso de corte

de la energía, le proporcionaría una autonomía al sistema de entre 12 horas y 3 días (dependiendo de la capacidad de la batería).

Los modelos disponibles de centrales, parten de una base de 4 zonas y existen modelos hasta 128 zonas. Los modelos multiplexados (Particiones) permiten a partir de cuatro cables particionar una central de alarma funcionando la misma como si fueran dos o cuatro centrales independientes.

### **Detector de Humo**



Un detector de humo es un aparato de seguridad que detecta la presencia de humo en el aire y emite una señal acústica avisando del peligro de incendio. Atendiendo al método de detección que usan pueden ser de varios tipos: - Detectores iónicos: Utilizados para la detección de gases y humos de combustión que no son visibles a simple vista. - Detectores de humos: Detectan los humos visibles mediante la absorción o difusión de la luz.

Pueden ser de dos tipos, según detecten el humo por oscurecimiento o por dispersión del aire en un espacio:

- De rayo infrarrojo, compuestos por un dispositivo emisor y otro receptor. Cuando se oscurece el espacio entre ellos debido al humo sólo una fracción de la luz emitida alcanza al receptor provocando que la señal eléctrica producida por éste sea más débil y se active la alarma.
- De tipo puntual, en los que emisor y receptor se encuentran alojados en la misma cámara pero no se ven al formar sus ejes un ángulo mayor de 90° y estar separados por una pantalla, de manera que el rayo emitido no alcanza el receptor. 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.

## Infrarrojos Pasivos



Los infrarrojos pasivos detectan el movimiento de los cuerpos que desprenden calor y rayos infrarrojos (a través de un sensor piro eléctrico y por medio de un lente de fresnell que concentra los rayos infrarrojos hacia el sensor). La capacidad de cobertura es de 12 mts y 90° aunque también existen con cobertura de 360°.

Los sensores infrarrojos DOBLE TECNOLOGÍA poseen características propias de combinación de la tecnología infrarroja y volumétrica, se emplean para evitar falsas alarmas ya que para activarse deberán funcionar ambas tecnologías.



Detector de movimiento lunar útil para supermercados o bodegas

## Teclado lcd icon



El teclado es el dispositivo que permite realizar las programaciones de la central de alarma así como también realizar el control del sistema como activación, desactivación, cancelación de zonas, etc.

Es el elemento más común y fácil de identificar en una alarma. Se trata de un teclado numérico del tipo telefónico. Su función principal es la de permitir a los usuarios autorizados (usualmente mediante códigos preestablecidos) armar (activar) y desarmar (desactivar) el sistema. Además de esta función básica, el teclado puede tener botones de funciones como: Emergencia Médica, Intrusión, Fuego, etc. Por otro lado, el teclado es el medio más común mediante el cual se configura el panel de control.

Dentro de la programación se realizarán tales como programación de claves, tiempos entrada, salida duración de la sirena, y diferentes tipos de zonas como ser perimetral, interna, temporizada, etc.

Los teclados podrán ser con leds (luces) indicadores o con display alfanumérico que a través del mismo se visualizarán palabras con indicaciones de fácil lectura.

Un sistema podrá disponer de más de un teclado como también podrá conectarse un control remoto para realizar activaciones y desactivaciones a distancia.

### Teclado 1555 LED Para los paneles DSC



## Batería de gel libre de mantenimiento de 4 o 7 Amperios 12 voltios



La batería es utilizada para darle respaldo eléctrico al sistema, en caso de fallas en el suministro de energía, este puede ser de entre 12 horas hasta de 72 horas dependiendo del tipo y estado.

## Sirena electrónica de 30 a 15 Vatios 12 Voltios



Es el mecanismo más efectivo que el sistema tiene para alertar sobre una novedad en el funcionamiento del mismo.

Esta tiene varios sonidos para alertar sobre el tipo de novedad presentada.

Ej. Sonido continuo, para alertar sobre intrusión.

Sonido intermitente, para alertar sobre Fuego.

## Detectores magnéticos.

Suiche Magnético Liviano para puertas. Ventanas o cajones o cajas fuertes.



Se trata de un sensor que forma un circuito cerrado por un imán y un contacto muy sensible que al separarse, cambia el estado (se puede programar como NC o NA) provocando un salto de alarma. Se utiliza en puertas y ventanas, colocando una parte del sensor en el marco y otra en la puerta o ventana misma.



Los swiches son dispositivos que estarán ubicados en el marco de las aberturas (puertas, ventanas) y a través de un Magnético permitirán detectar la abertura del lugar controlado.

#### **Pulsadores de asalto (Botón de Pánico).**



Son solo pulsadores de alarma de contactos secos que permitirá activar el sistema sin que suene la sirena en caso de asalto. Se podrán instalar en los baños, bajo mesas, etc.

También lo hay como receptor con llavero inalámbrico, puede ser utilizado como botón de pánico o activar desactivar la alarma.



Receptora inalámbrica para Botones de pánico o accesorios inalámbricos.

### **Detectores de ruptura de vidrio acústicos.**



Estos dispositivos detectan la rotura de vidrios a través de un micrófono incorporado que censa las frecuencias de sonido, la rotura de vidrios producen una frecuencia de sonido muy particular con picos de sensibilidad muy altos, al ser detectados por el sensor este enviará a a la central la condición de alarma. La capacidad de cobertura es de 8 mts.

Son detectores microfónicos, activados al detectar la frecuencia aguda del sonido de una rotura de cristal.

### **Sensores inerciales o sísmicos.**

Son Aparatos (Mecanismos) preparados para detectar golpes sobre una base. Se colocan especialmente en cajas fuertes, también en puertas, paredes y ventanas. Detectan el intento de forzar su apertura.

### **Gabinete de sirena exterior.**

Es el elemento más visible desde el exterior del inmueble protegido. Se trata de una sirena con autonomía propia (puede funcionar aún si se le corta el suministro de corriente alterna o si se pierde la comunicación con la central procesadora) colocada dentro de un gabinete protector (de metal, policarbonato, etc.). Puede tener además diferentes sistemas luminosos que funcionan en conjunto con la disuasión sonora.

### **Detector de movimiento sencillo inalámbrico**



Diversos tipos de captadores o sensores:

- Sensores de luz
  - Elementos sensibles
  - LDRs o Fotorresistores (resistores variables por la incidencia de la luz)
  - Foto celdas o celdas fotovoltaicas
  - Fotodiodos
  - Fototransistores
  - CCD
  - Cámaras de vídeo
- Módulos integrados
  - Reflectivo
  - De ranura

- Sensores de presión y fuerza
  - Elementos sensibles
  - Microinterruptores o Sensores de presión o Sensores de fuerza
  - Sensores
  - Sensores de contacto (sándwich, bigotes, antenas)
  - Piel robótica
  
- Sensores de sonido
  - Elementos sensibles
  - Micrófonos
  - Captadores piezoeléctricos

## j. Sistema de comunicación y enlace

### SISTEMA DE COMUNICACIÓN Y ENLACE

#### Modelo de un Sistema de Comunicaciones :

La Comunicación es la transferencia de información con sentido desde un lugar (remitente, origen, fuente, transmisor) a otro lugar (destino, receptor). Por otra parte Información es un patrón físico al cual se le ha asignado un significado comúnmente acordado. El patrón debe ser único (separado y distinto), capaz de ser enviado por el transmisor, y capaz de ser detectado y entendido por el receptor.

Si la información es intercambiada entre comunicadores humanos, por lo general se transmite en forma de sonido, luz o patrones de textura en forma tal que pueda ser detectada por los sentidos primarios del oído, vista y tacto. El receptor asumirá que no se está comunicando información si no se reciben patrones reconocibles.

En la siguiente figura se muestra un diagrama a bloques del modelo básico de un sistema de comunicaciones, en éste se muestran los principales componentes que permiten la comunicación.



Elementos básicos de un sistema de comunicaciones

## ELEMENTOS DEL SISTEMA

En toda comunicación existen tres elementos básicos (imprescindibles uno del otro) en un sistema de comunicación: el transmisor, el canal de transmisión y el receptor. Cada uno tiene una función característica.

**El Transmisor** pasa el mensaje al canal en forma de señal. Para lograr una transmisión eficiente y efectiva, se deben desarrollar varias operaciones de procesamiento de la señal. La más común e importante es la modulación, un proceso que se distingue por el acoplamiento de la señal transmitida a las propiedades del canal, por medio de una onda portadora.

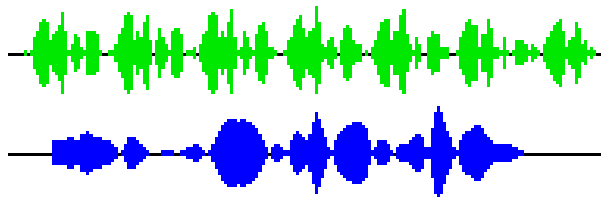
**El Canal de Transmisión** o medio es el enlace eléctrico entre el transmisor y el receptor, siendo el puente de unión entre la fuente y el destino. Este medio puede ser un par de alambres, un cable coaxial, el aire, etc. Pero sin importar el tipo, todos los medios de transmisión se caracterizan por la atenuación, la disminución progresiva de la potencia de la señal conforme aumenta la distancia.

**La función del Receptor** es extraer del canal la señal deseada y entregarla al transductor de salida. Como las señales son frecuentemente muy débiles, como resultado de la atenuación, el receptor debe tener varias etapas de amplificación. En todo caso, la operación clave que ejecuta el receptor es la demodulación, el caso inverso del proceso de modulación del transmisor, con lo cual vuelve la señal a su forma original.

**El Mensaje** Información que se pretende llegue del emisor al receptor por medio de un sistema de comunicación. Puede ser en formas como ser texto, número, audio, gráficos, etc. Este también puede ser de forma verbal o no verbal.

### Tipos de Señal

**Señal análoga:** Usa variaciones (modulaciones) en una señal, para enviar información. Es especialmente útil para datos en forma de ondas como las ondas del sonido. Las señales análogas son las que usan normalmente su línea de teléfono y sus parlantes.



Las señales análogas se pueden modular en:

**Amplitud Modulada:** Se emplean dos niveles diferentes de voltajes para representar el 0 y el 1 respectivamente.

**Frecuencia Modulada:** Se utilizan dos o más tonos diferentes.

**Señal Digital:** Es una corriente de 0 y 1 toman un conjunto finito de valores en un intervalo de interés.

La señal digital se puede modular por:

### **Modulación por Impulsos Codificados MIC**

#### **Pulse Coded Modulation (PCM)**

Cuando se habla por teléfono sale una señal análoga normal que después se digitaliza mediante un **Codec** produciendo un número de 7 u 8 bits. El Codec efectúa 8000 muestras por segundo (125 s /muestra) con este número de muestras es suficiente para capturar toda la información de un ancho de banda de 4Khz.

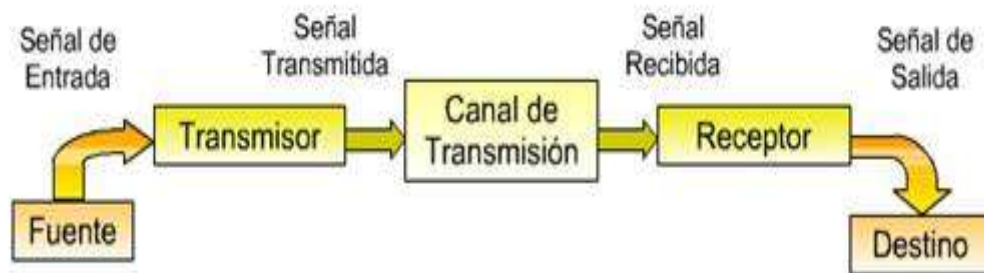
### **Tipos de Transmisión**

**Serie:** Transmisión sobre un canal de una sola línea, la mayoría de las redes de comunicaciones utilizan la transmisión en serie entre terminales y computadoras. En la transmisión serie los bits van uno detrás de otro a través de un cable. Se requiere de una sincronización.

**Paralelo:** Los datos pueden transmitirse entre ordenadores y terminales mediante cambios de corriente o tensión en un cable, salen un grupo de bits a la vez por varias líneas (Se puede decir que el paralelo es la unión de varias series), o sea cada bit de un carácter se traslada por su propio cable.

Hay una señal llamada **Strobe** o reloj que va sobre un cable adicional e indica al receptor cuando están presentes todos los bits sobre sus respectivos cables para que se pueda tomar una muestra de valores.

La comunicación en paralelo es útil a corta distancia, siendo más rápida.



### Contaminaciones de la señal

Durante la transmisión de la señal ocurren ciertos efectos no deseados. Algunos de ellos son la atenuación, distorsión, la interferencia y el ruido, los cuales se manifiestan como alteraciones de la forma de la señal. Al introducirse estas contaminaciones al sistema, es una práctica común y conveniente imputárselas, pues el transmisor y el receptor son considerados ideales. En términos generales, cualquier perturbación no intencional de la señal se puede clasificar como "ruido", y algunas veces es difícil distinguir las diferentes causas que originan una señal contaminada. Existen buenas razones y bases para separar estos tres efectos, de la manera siguiente:

**Atenuación:** Desgaste que sufre la señal de energía ocasionada por la distancia entre el emisor y el receptor. Toda señal eléctrica al ser transmitida por un medio físico o por espacio experimenta una pérdida de potencia denominada atenuación. Se mide normalmente en decibelios por unidad de distancia

**Distorsión:** Es la deformación que experimenta la señal al ser transmitida por un canal debida a la respuesta imperfecta del sistema a ella misma. A diferencia del ruido y la interferencia, la distorsión desaparece cuando la señal deja de aplicarse.

**Interferencia:** Es la contaminación por señales extrañas, generalmente artificiales y de forma similar a las de la señal. El problema es particularmente común en emisiones de radio, donde pueden ser captadas dos o más señales simultáneamente por el receptor. La solución al problema de la interferencia es obvia; eliminar en una u otra forma la señal interferente o su fuente. En este caso es posible una solución perfecta, sí bien no siempre práctica.

**Ruido:** Interferencia externa sobre la señal transmitida. Por ruido se debe de entender las señales aleatorias e impredecibles de tipo eléctrico originadas en forma natural dentro o fuera del sistema. Cuando estas señales se agregan a la señal portadora de la información, ésta puede quedar en gran parte oculta o eliminada totalmente. Por supuesto que podemos decir lo mismo en relación a la interferencia y la distorsión y en cuanto al ruido que no puede ser eliminado nunca completamente, ni aún en teoría.

### **Frecuencias de transmisión**

Frecuencias extremadamente bajas: Llamadas ELF (Extremely Low Frequencies), son aquellas que se encuentran en el intervalo de 3 a 30 Hz. Este rango es equivalente a aquellas frecuencias del sonido en la parte más baja (grave) del intervalo de percepción del oído humano. Cabe destacar aquí que el oído humano percibe ondas sonoras, no electromagnéticas, sin embargo se establece la analogía para poder hacer una mejor comparación. Frecuencias súper bajas: SLF (Super Low Frequencies), son aquellas que se encuentran en el intervalo de 30 a 300 Hz. En este rango se incluyen las ondas electromagnéticas de frecuencia equivalente a los sonidos graves que percibe el oído humano típico.

Frecuencias ultra bajas: ULF (Ultra Low Frequencies), son aquellas en el intervalo de 300 a 3000 Hz. Este es el intervalo equivalente a la frecuencia sonora normal para la mayor parte de la voz humana.

Frecuencias muy bajas: VLF, Very Low Frequencies. Se pueden incluir aquí las frecuencias de 3 a 30 kHz. El intervalo de VLF es usado típicamente en comunicaciones gubernamentales y militares.

Frecuencias bajas: LF, (Low Frequencies), son aquellas en el intervalo de 30 a 300 kHz. Los principales servicios de comunicaciones que trabajan en este rango están la navegación aeronáutica y marina.

Frecuencias medias: MF, Medium Frequencies, están en el intervalo de 300 a 3000 kHz. Las ondas más importantes en este rango son las de radiodifusión de AM (530 a 1605 kHz).

Frecuencias altas: HF, High Frequencies, son aquellas contenidas en el rango de 3 a 30 MHz. A estas se les conoce también como "onda corta". Es en este intervalo que se tiene una amplia gama de tipos de radiocomunicaciones como radiodifusión, comunicaciones gubernamentales y militares. Las

comunicaciones en banda de radioaficionados y banda civil también ocurren en esta parte del espectro.

Frecuencias muy altas: VHF, Very High Frequencies, van de 30 a 300 MHz. Es un rango popular usado para muchos servicios, como la radio móvil, comunicaciones marinas y aeronáuticas, transmisión de radio en FM (88 a 108 MHz) y los canales de televisión del 2 al 12 [según norma CCIR (Estándar B+G Europa)]. También hay varias bandas de radioaficionados en este rango.

Frecuencias ultra altas: UHF, Ultra High Frequencies, abarcan de 300 a 3000 MHz, incluye los canales de televisión de UHF, es decir, del 21 al 69 [según norma CCIR (Estándar B+G Europa)] y se usan también en servicios móviles de comunicación en tierra, en servicios de telefonía celular y en comunicaciones militares.

Frecuencias super altas: SHF, Super High Frequencies, son aquellas entre 3 y 30 GHz y son ampliamente utilizadas para comunicaciones vía satélite y radioenlaces terrestres. Además, pretenden utilizarse en comunicaciones de alta tasa de transmisión de datos a muy corto alcance mediante UWB. También son utilizadas con fines militares, por ejemplo en radares basados en UWB.

Frecuencias extremadamente altas: EHF, Extremely High Frequencies, se extienden de 30 a 300 GHz. Los equipos usados para transmitir y recibir estas señales son más complejos y costosos, por lo que no están muy difundidos aún.

### **Espectro electromagnético**

Se denomina espectro electromagnético a la distribución energética del conjunto de las ondas electromagnéticas. Referido a un objeto se denomina espectro electromagnético o simplemente espectro a la radiación electromagnética que emite (espectro de emisión) o absorbe (espectro de absorción) una sustancia. Dicha radiación sirve para identificar la sustancia de manera análoga a una huella dactilar. Los espectros se pueden observar mediante espectroscopios que, además de permitir observar el espectro, permiten realizar medidas sobre el mismo, como son la longitud de onda, la frecuencia y la intensidad de la radiación.

El espectro electromagnético se extiende desde la radiación de menor longitud de onda, como los rayos gamma y los rayos X, pasando por la luz ultravioleta, la luz visible y los rayos infrarrojos, hasta las ondas electromagnéticas de mayor longitud de onda, como son las ondas de radio. Se cree que el límite para la longitud de onda más pequeña posible es la longitud de Planck mientras

que el límite máximo sería el tamaño del Universo (véase Cosmología física) aunque formalmente el espectro electromagnético es infinito y continuo.

### **Onda electromagnética**

Una onda electromagnética es la forma de propagación de la radiación electromagnética a través del espacio. Y sus aspectos teóricos están relacionados con la solución en forma de onda que admiten las ecuaciones de Maxwell. A diferencia de las ondas mecánicas, las ondas electromagnéticas no necesitan de un medio material para propagarse; es decir, pueden desplazarse por el vacío.

### **Longitud de onda**

La **longitud de una onda** es el período espacial de la misma, es decir, la distancia que hay de pulso a pulso. Normalmente se consideran dos puntos consecutivos que poseen la misma fase: dos máximos, dos mínimos, dos cruces por cero (en el mismo sentido)

### **Frecuencia**

Frecuencia es una magnitud que mide el número de repeticiones por unidad de tiempo de cualquier fenómeno o suceso periódico.

Para calcular la frecuencia de un suceso, se contabilizan un número de ocurrencias de este teniendo en cuenta un intervalo temporal, luego estas repeticiones se dividen por el tiempo transcurrido. Según el Sistema Internacional (SI), la frecuencia se mide en hercios (Hz), en honor a Heinrich Rudolf Hertz. Un hercio es la frecuencia de un suceso o fenómeno repetido una vez por segundo. Así, un fenómeno con una frecuencia de dos hercios se repite dos veces por segundo. Esta unidad se llamó originariamente «ciclo por segundo» (cps) y aún se sigue utilizando. Otras unidades para indicar la frecuencia son revoluciones por minuto (rpm). Las pulsaciones del corazón y el tempo musical se miden en «pulsos por minuto» (bpm, del inglés beats per minute).

$$1 \text{ Hz} = \frac{1}{\text{s}}$$

## **Equipos de Comunicación**

Los equipos de comunicación permiten comunicarse con otras personas que se encuentran lejos, dentro de los equipos más comunes se tienen:

Teléfono fijo, móvil, celular, equipos de radio, transmisor y receptor, la televisión digital.

La PC con conexión a Internet, comunicación por correo, video, voz y datos, estos se transmiten por un medio, ya sea físico o por el aire.

En el caso físico se transmiten por cables de cobre, coaxiales, fibra óptica, etc. Si es por aire se transmiten por ondas de radio (microondas)

## **Equipos de Comunicación**

- RADIO KENWOOD TK5160
- RADIO MOVIL KENWOOD TK-7160HK/TK-8190
- RADIO PORTATIL KENWOOD TK-2202/TK-3202
- RADIO TELEFONO MOTOROLA PRO3100
- RADIO TELEFONO PORTATIL EP450
- RADIO MOVIL ICOM A24
- RADIO MOVIL ICOM IC-F121S
- RADIO TELEFONO EM400
- RADIO KENWOOD TK 5160
- RADIO MOVIL KENWOOD TK-7160HK / TK-8190HK
- RADIO PORTATIL KENWOOD TK-2202 / TK-3202
- RADIO TELEFONO MOTOROLA PRO3100
- RADIO TELEFONO EM400
- RADIO TELEFONO PORTATIL EP450
- RADIO ICOM IC A24
- RADIO MOVIL ICOM IC-F121S

## **Equipos Base**

Equipos de VHF y UHF para uso comercial y radioaficionados, nuevos y usados; repetidoras, móviles para remis, taxi, ambulancias, etc.

## **Equipos de mano**

Handys VHF y UHF para uso comercial y radioaficionado, nuevo y usado. Handys, equipos de uso simple o con repetidora

### **Antenas fijas**

Antenas para distintas bandas. Nacionales y de fabricación propia. Formación de dipolos para repetidoras. Antenas para enlaces.

### **Fuentes y cargadores**

Fuentes de alimentación nueva y usada. Fabricación y reparación.

### **Duplexores**

Duplexores para enlaces y repetidoras. Fabricados de acuerdo al pedido y a las frecuencias solicitadas.

### **Baterías**

Packs de baterías para los diferentes modelos de equipos de mano. Con todos los repuestos

### **Cámaras y CCTV**

Cámaras para interior y exterior. Grabadoras digitales, lentes, conversores y soportes.

### **Micrófonos Handys**

Línea de corbateros, laringófonos, parlantes para todas las marcas y modelos de handies.

### **Alarmas X-28**

Alarmas para viviendas, instalación y mantenimiento. Sensores, bocinas, llaveros, teclados, etc.

Equipos y accesorios para cubrir las necesidades:

- Equipos de radiocomunicaciones para exposiciones.
- Equipos de radiocomunicaciones para carreras de autos.
- Equipos de radiocomunicaciones para recitales y shows.
- Equipos de seguridad, cobertura de eventos especiales, etc.

### **Equipos de Comunicación**

Un módem (Modulador – Demodulador) es un dispositivo Módems que convierte las señales digitales del computador en señales analógicas que

pueden transmitirse a través del canal telefónico. Características Es un dispositivo que sirve para modular y desmodular una señal. El modulador emite una señal sinusoidal denominada portadora. La señal moduladora constituye la información que se prepara para una transmisión. Un módem prepara la información para ser transmitida, pero no realiza la transmisión. La mayoría de los módem son full-dúplex, lo cual significa que pueden transferir datos en ambas direcciones. De las funciones, Modulación y Demodulación, surgió el nombre del módem. Ventajas • El módem es uno de los métodos más extendidos para la interconexión de computadores por su sencillez y bajo costo.

Funciona en el nivel físico del modelo de referencia OSI para Repetidor regenerar las señales de la red y reenviarla a otros segmentos Características Es un elemento que permite la conexión de dos Segmentos de red no traducen o filtran señales Sólo nos permite extender la longitud física de una red, por lo tanto no cambia de ninguna forma la funcionalidad de la red. Crea una copia más fiable de la trama. Un repetidor no es un amplificador. Cuando se utilizan repetidores para extender la red, no olvide la regla 5-4-3.

#### Ventajas

- Incrementa la distancia cubierta por la LAN
- Retransmite los datos sin retardos.
- Es transparente a los niveles superiores al físico Desventajas
- Repetidor y dominio de colisión

Es regenerar y retemporizar las señales de Hub red, utilizando un proceso denominado concentración Características hub también se denomina repetidor multipuerto. Las razones por las que se usan los hubs son crear un punto de conexión central para los medios de cableado y aumentar la confiabilidad de la red los hubs se especifican en activos o pasivos e Inteligentes y no inteligentes Clasificación Grupo de Trabajo Intermedio Principal Ventajas • Punto de conexión central • Conocido como HUB asociado al estándar IOBaseT • El paquete transmitido se repite hacia todos los puertos Desventajas • Dominio de colisión • es vulnerable

Gateway (Compuerta-pasarela) Una pasarela consiste en una computadora u otro dispositivo que actúa como traductor entre dos sistemas que no utilizan los mismos protocolos de comunicaciones, formatos de estructura de datos, lenguajes y/o arquitecturas. Una pasarela no es como un puente, que simplemente transfiere la información entre dos sistemas sin realizar conversión. Una pasarela modifica el empaquetamiento de la información o su sintaxis para acomodarse al sistema destino. Su trabajo está dirigido al nivel más alto de la referencia OSI Los gateways tienen mayores capacidades que

los routers y los bridges porque no sólo conectan redes de diferentes tipos, sino que también aseguran que los datos de una red que transportan son compatibles con los de la otra red. Conectan redes de diferentes arquitecturas procesando sus protocolos y permitiendo que los dispositivos de un tipo de red puedan comunicarse con otros dispositivos de otro tipo de red.

## k. Radiocomunicaciones

La radio digital es un tipo de radios que tramite información en forma de señal digital utilizando un método denominado modulación digital. Una forma de radio digital de alta definición (HD, por sus siglas en inglés) proporciona una mejor calidad de sonido. La radio por Internet transmite información en directo a través de computadoras en línea, mientras que la radio satelital hace uso de señales digitales transmitidas vía satélite. Cualquier persona puede hacer uso de cientos de estaciones de música y noticias las 24 horas al día, los siete días de la semana sin interrupciones comerciales. Los usuarios compran equipos y configuran las cuentas con el proveedor de servicio. La Banda ciudadana (BC, por sus siglas en inglés) es un tipo de comunicación de radio de dos vías que fue muy popular en la década de 1970 y es comúnmente utilizado por los camioneros. Los CB permiten que las personas se comuniquen entre sí mediante el uso de 40 canales de alta frecuencia (HF, por sus siglas en inglés) sobre AM y SSB. El walkie – talkie es un tipo radio de mano que tiene un receptor y un transceptor como un dispositivo de CB, sólo que este portátil y tiene un menor alcance. Distintas personas se comunican como un pasatiempo por diversión y pueden aprender a utilizar la radio “Ham”, también conocida como radio para aficionados.



El reglamento de radiocomunicaciones, que es el tratado internacional por el cual se rife la utilización del espectro de frecuencias radioeléctricas y de las órbitas de los satélites geoestacionarios y no geoestacionarios. Las modificaciones se realizan sobre la base de un orden del día determinado por el Consejo de la UIT, que tiene en cuenta las recomendaciones formuladas por las conferencias mundiales de radiocomunicaciones anteriores.

Los temas generales del orden del día de las conferencias mundiales de radiocomunicaciones se determinan con una antelación de cuatro a seis años, y el Consejo de UIT establece el orden del día final dos años antes de la conferencia con el acuerdo de la mayoría de los Estados Miembros.

De conformidad con la Constitución de la UIT, la CMR podrá:

Revisar el Reglamento de Radiocomunicaciones y cualquiera de los Planes correspondientes de Asignación y Adjudicación de Frecuencia.

Examinar cualquier asunto de radiocomunicaciones de carácter mundial.

Formular instrucciones dirigidas a la Junta del Reglamento de Radiocomunicaciones y a la Oficina de Radiocomunicaciones, y revisar sus actividades.

Determinar las Cuestiones que han de ser objeto de estudio por la Asamblea de Radiocomunicaciones y sus Comisiones de Estudio, como parte de los trabajos preparatorios para futuras Conferencias de Radiocomunicaciones.

Basándose en las contribuciones de las administraciones, de la Comisión Especial, las Comisiones de Estudio de Radiocomunicaciones y de otras fuentes relacionadas con los temas reglamentarios, técnicos, de explotación y de procedimiento que examinarán las Conferencias Mundiales y Regionales de Radiocomunicaciones (véase el Artículo 19 del Convenio (Ginebra, 1992), la Reunión Preparatoria de Conferencias (RPC) preparará un informe refundido que se utilizará como base para el trabajo de dichas conferencias.

El Reglamento de Radiocomunicaciones contiene el texto completo de Reglamento de Radiocomunicaciones adoptado por la Conferencia Mundial de Radiocomunicaciones (Ginebra, 1995) (CMR – 95) y ulteriormente revisado y adoptado por las conferencias Mundiales de Radiocomunicaciones, junto con todos los Apéndices, las Resoluciones, las Recomendaciones y las Recomendaciones UIT – R incorporadas por referencia.

## **Reglamento de Radiocomunicaciones**

### **Edición de 2012**

El texto completo del Reglamento de Radiocomunicaciones (RR), adoptado por la CMR-95 y ulteriormente revisado y adoptado por la CMR-97, por la CMR-2000, por la CMR-03, por la CMR-07 y por la CMR-12, se publica en cuatro volúmenes junto con una serie separada con los mapas que deben ser utilizados en el Apéndice 27 (Rev.CMR-12).

A continuación se resume el contenido de la publicación:

VOLUMEN 1 – ARTÍCULOS

VOLUMEN 2 – APÉNDICES

VOLUMEN 3 – RESOLUCIONES Y RECOMENDACIONES

VOLUMEN 4 – RECOMENDACIONES UIT-R INCORPORADAS POR REFERENCIA

SERIE SEPARADA – MAPAS QUE DEBEN SER UTILIZADOS EN EL APÉNDICE 27 (REV.CMR-12)

#### FORMATO Y ESTRUCTURA

Copia impresa: Cuatro volúmenes en formato A5 (21 - 4,8 cm) únicamente, junto con la serie separada de los mapas que deben ser utilizados en el Apéndice 27 (Rev.CMR-12).

Véanse las «Directrices relativas al uso de las versiones electrónicas (Photoshop) de los transparentes (hojas de cálculo) asociados a los mapas del Apéndice 27 (Rev.CMR-12)».

DVD-ROM: Microsoft® Office Word 9.0 y Adobe® Acrobat® PDF.

Librería electrónica: Microsoft® Office Word 9.0 o Adobe® Acrobat® PDF.

#### **Servicios Espaciales (SSD)**

Aplica los procedimientos internacionales de coordinación, notificación y registro para los sistemas espaciales y las estaciones terrenas, que determinan el reconocimiento internacional a través de la inclusión en el Registro Internacional de Frecuencias.

Gestiona los procedimientos de la UIT en materia de asignación y atribución relacionados con el espacio y proporciona asistencia al respecto a todas las partes interesadas de la UIT

El Departamento de Servicios Espaciales (SSD) es responsable de los procedimientos de coordinación e inscripción de los sistemas espaciales y las estaciones terrenas. El Departamento se encarga de la recopilación, procesamiento y publicación de los datos y lleva a cabo exámenes de las notificaciones de asignaciones de frecuencias presentadas por las administraciones para su inclusión en los procedimientos de coordinación formales o su inscripción en el Registro Internacional de Frecuencias (MIFR).

El Departamento también es responsable de controlar los procedimientos de los planes de asignaciones o adjudicaciones espaciales correspondientes de la UIT y de prestar asistencia a las administraciones sobre los temas antes indicados.

#### Estructura del SSD

- División de publicaciones y registro de servicios espaciales (SPR)
- División de coordinación de sistemas espaciales (SSC)
- División de notificación y planes de servicios espaciales (SNP)

#### BR IFIC y Prefacio

La Circular Internacional de Información sobre Frecuencias (Servicios espaciales) (BR IFIC) es un documento de servicio en formato de DVD-ROM, publicado cada dos semanas.

El Prefacio (Servicios espaciales) describe el contenido y estructura de la Circular BR IFIC. Más

#### SNL En línea

La lista de redes de satélite (SNL) es un grupo de datos relativos a las estaciones espaciales, las estaciones terrenas y las estaciones de radio astronomía planificadas o existentes. Contiene información sobre la utilización del espectro, la ocupación de las órbitas, las publicaciones de referencia y redes pendientes

#### Planes Espaciales

Información relativa a las redes de satélite en las bandas planificadas y en particular a las disposiciones para los servicios espaciales planificados que figuran en los Apéndices 30, 30A y 30B del Reglamento de Radiocomunicaciones

### Soporte

Información sobre las notificaciones en formato electrónico, publicaciones, bases de datos, seminarios y talleres de la Oficina de Radiocomunicaciones

### SNS En línea

El Sistema de Redes Espaciales en línea permite el acceso a la base de datos SNS de la Oficina de Radiocomunicaciones. Proporciona los datos SNS de redes de satélite planificadas y no planificadas. Se necesita una cuenta TIES o una suscripción para acceder al servicio

## **SERVICIOS TERRENALES**

Aplica los procedimientos internacionales de coordinación, notificación y registro para los servicios terrenales, que determinan el reconocimiento internacional a través de la inclusión en el Registro Internacional de Frecuencias y en los Planes.

Aplica los procedimientos administrativos que tratan de la atribución de medios de identificación internacionales (Series de distintivos de llamada, MID), y mantiene las bases de datos marítimas de la UIT relacionadas con la seguridad de la vida

### **Equipos de radio**

La radiocomunicación tradicional para radios de dos vías es el instrumento favorito de aquellos que requieren una comunicación instantánea y económica.

### **Beneficios de la Radiocomunicación**

- Mantener comunicación con personas relevantes a los procesos de tu empresa en forma sencilla y económica
- Contacto con una o varias personas con tan solo oprimir un botón.
- Comunicación eficiente inmediata ante cualquier imprevisto sin marcar números.
- Mejor control de tu presupuesto de comunicación

- Uso particularmente para motivos de trabajo
- Puedes usarlos todo el tiempo sin que haya costo por duración de llamada.
- Para su uso no ocupas adquirir saldos o hacer prepagos.

### **Soluciones por Industria**

Los sistemas de Radiocomunicación mejoran las comunicaciones generales en tu negocio ya sea para fines de seguridad, supervisión o bien como apoyo a los procesos operativos de tu empresa. Con los productos y servicios de radiocomunicación que ofrecemos obtienes una respuesta inmediata y mejoras la productividad por el mejor control sobre tus empleados, por ejemplo:

- Seguridad: con un sistema de radiocomunicación obtienes comunicación inmediata entre los vigilantes y con sus superiores para la prevención y el reporte de situaciones de rutina y o anormales.
- Comerciales: un sistema de radiocomunicación facilita la interacción entre las diferentes áreas del negocio para ofrecer una mejor respuesta al cliente como puede ser en materia de inventarios, vetas, embarques y servicios al cliente
- Turismo y hoteles: un sistema de radiocomunicación ofrece sistemas de seguridad de mayor valor para los huéspedes y mejores tiempos de respuesta en la atención de sus requerimientos.
- Empresas de Manufactura: con radiocomunicación optimizas el transporte de materiales al lugar de trabajo y facilita las comunicaciones entre las líneas de producción y los supervisores.

### **Función**

Los radios UHF y VHF son radios de dos vías UHF por siglas en inglés, significa frecuencia ultra alta y VHF frecuencia muy alta. Un radio de dos vías es algo como un walkie – talkie, aunque hay varias diferencias entre un conjunto simple de walkie – talkie y un radio UHF o VHF. El mayor de estos es el alcance y las frecuencias de los tres.

### **UHF**

De 300 a 3000 MHz (mega Hertz) las frecuencias representan las radios de rango de UHF (Frecuencia Ultra Alta). Ahora se ha vuelto posible y fácil de crear y construir un radio de dos vías con esta capacidad de frecuencia. Debido a esto, los radios UHF se han vuelto más económicos de comprar y han entrado en competencia directa con radios VHF. De hecho, UHF se considera ser más

popular que los radios VHF. Radios de UHF se utilizan comúnmente en interiores o en áreas donde se puede encontrar mucha interferencia, tales como edificios y colinas. Se sabe que tienen un menor rango de distancia al aire libre, pero se sabe que pueden pasar a través de acero, madera y otros materiales de construcción.

### VHF

Los radios VHF utilizan frecuencias desde 30 a 300 MHz. Recuerda, que VHF es sinónimo de muy alta frecuencia. Estos radios funcionan mejor en ambientes al aire libre y con poco que obstruya la señal. Por estas razones, los radios VHF se utilizan a menudo en la configuración de la seguridad pública, tales como con seguridad al aire libre y situaciones de línea de visión. Las señales VHF viajan más lejos que UHF, pero de nuevo, no puede penetrar obstrucciones de la forma que los UHF lo hacen.