OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD

Estamos por comenzar !!!!

# Clase Nro. 3


# Estrategias de Mitigación de Riesgos: Sistemas de Alarmas

# Qué le llama la atención de esta fotografía ?

ORGANISMO TÉCNICO DE CAPACITACIÓN

# ¿COMO PROTEJO MI EMPRESA?

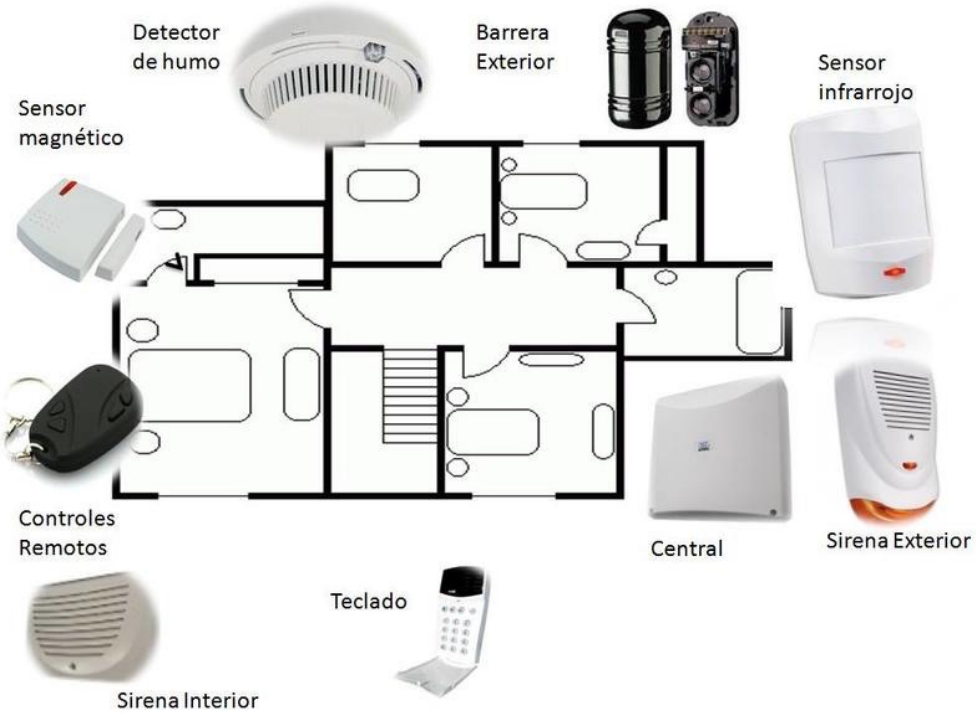
OTEC MSEREY
CENTRO DE ESTUDIO DE SEGURIDAD

**¿Qué quiero proteger?**
**Dinero, productos, personas, imagen etc.**

**De qué lo quiero proteger?**
**Cuales Amenazas hay entorno a la actividad?**

**¿Cómo lo voy a proteger?**
**Con qué ?**

# ¿CON QUÉ PROTEJO MI EMPRESA ?



OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD

# FUNDAMENTOS DE DISEÑO DE UN SISTEMA DE SEGURIDAD

OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD

# PREMISA BASE

"Aunque otros factores tales como los presupuestos, la cultura y la política interna también importan, la base primaria de la estrategia de protección de activos de una organización siempre debería ser el riesgo”

Physical Security Principles.(2015) Michael E. Knoke. ASIS International.

OTEC MSEREY
CENTRO DE ESTUDIO DE SEGURIDAD

# CONCEPTOS DE DISEÑO EN UN PPS

## DISEÑO EN PROFUNDIDAD

- El adversario debe derrotar o evitar capas o dispositivos sucesivos para lograr su objetivo.
- Obliga al usuario a prepararse más y usar más recursos.
- Consiste en complejizar el ataque.

## CONSECUENCIA MINIMA EN CASO DE FALLA

- Conocer los posibles tipos de fallas, ambientales, técnicas, capacidad de los adversarios.
- Contar con medidas de contingencia: Técnicas, procedimentales, humanas.

## SEGURIDAD BALANCEADA

- Mismo nivel de protección (detección y retardo) en todas las rutas de ataque = utopía.
- El sistema es tan fuerte como el más débil de los elementos.
- Proteger contra todas las amenazas en todas las rutas tomando manteniendo el equilibrio con los costos, seguridad e infraestructura.

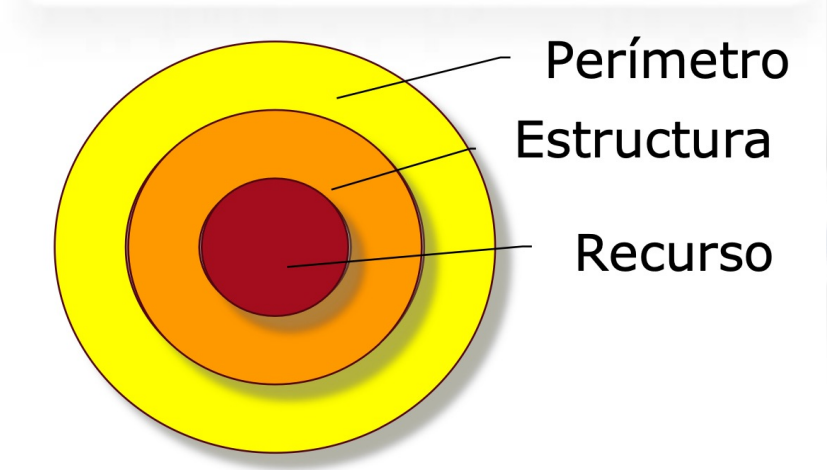
Asis International. (2012). “Protection of Assets, Physical Security”.

OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD

# DEFENSA EN PROFUNDIDAD

**Defensa en profundidad;** creando círculos concéntricos de contramedidas en el perímetro, estructura y recursos a proteger.



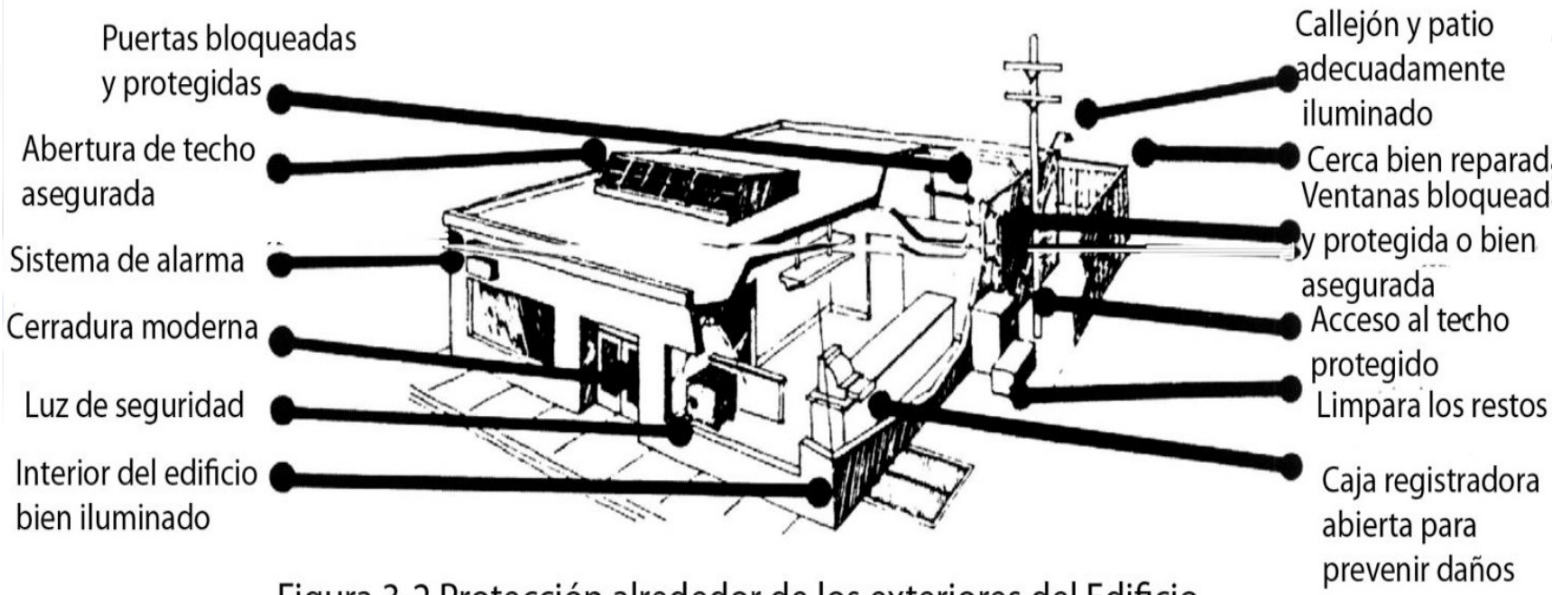




Figura 3-2 Protección alrededor de los exteriores del Edificio

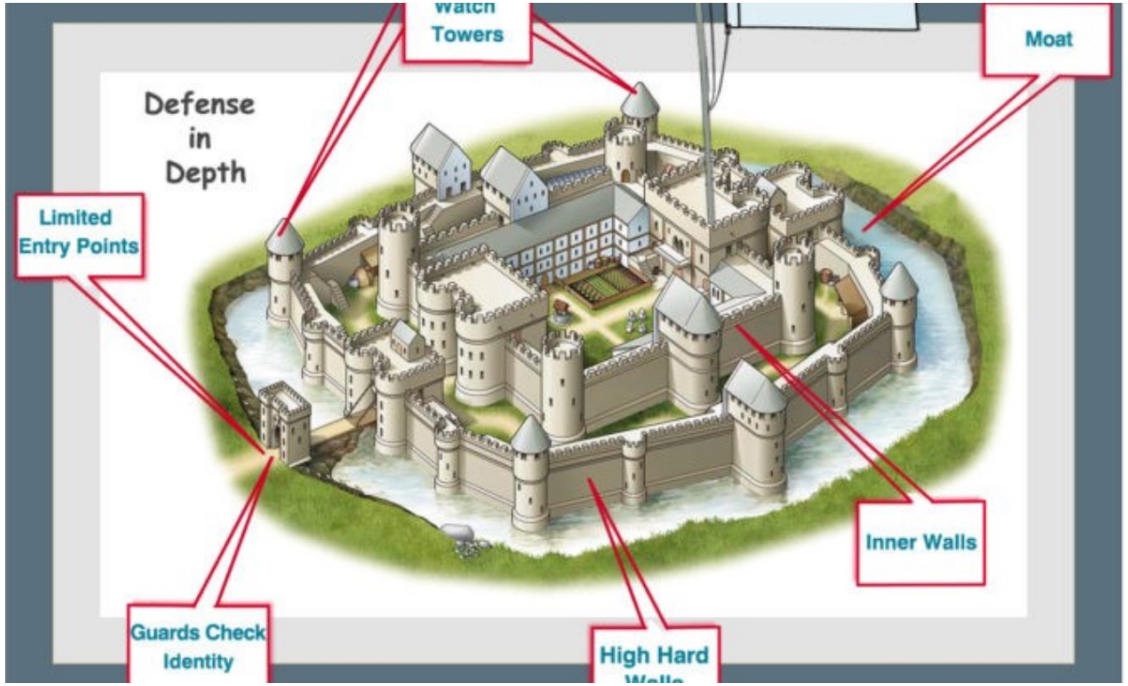
OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD

# DEFENSA EN PROFUNDIDAD

Deriva de la estrategia militar con el mismo nombre, y que está basada en la gestión del espacio como elemento de retraso y bloqueo del enemigo, y cuyo objetivo principal es frenar el avance de un ataque en lugar de derrotarlo con una sola línea de defensa fuerte.

Aplicado a sistemas actuales, se basa en la idea de que estas medidas de seguridad (capas) pueden crear problemas a los atacantes y de alguna forma frenarles en su avance a través de los sistemas.

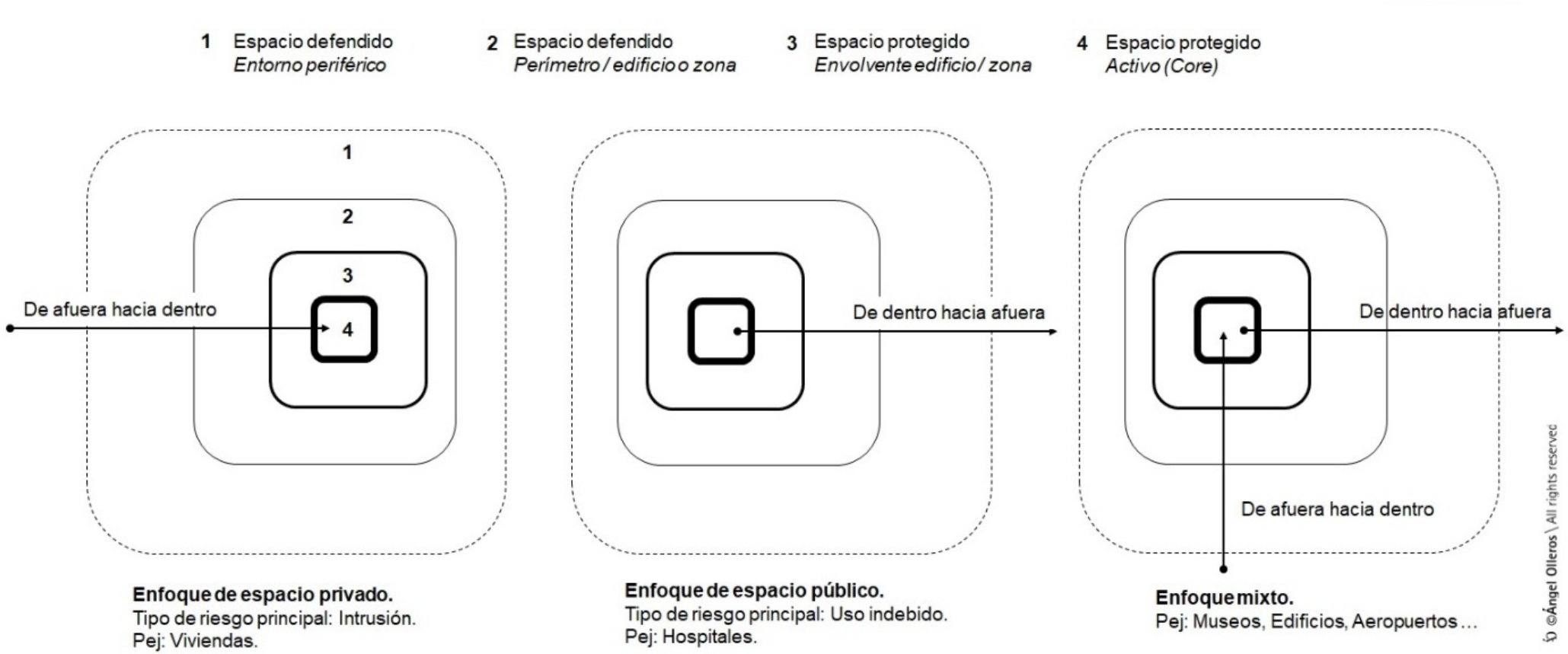



El “todo” genera mayor efectividad que la suma de las partes.

OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD

# DEFENSA EN PROFUNDIDAD CONSIDERANDO LA UTILIDAD DEL INMUEBLE



OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD

# ENFOQUES DE DISEÑO

**Desempeño**

**Características (cumplimiento)**

Evalúa desempeño o rendimiento de los elementos del sistema.

Efectividad de todos los elementos del sistema como un todo.

Permite determinar si hay mejoras en el desempeño

Evalúa Presencia de elementos

Efectividad = presencia de elementos

OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD


“Un diseño equilibrado del Sistema de Protección Física (SPF) integra las CUATRO categorías en cada punto de control.”

OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD

# CRITERIOS DE DISEÑO

- Detección
  - Probabilidad de detección
  - Tiempo para comunicar y evaluar
  - Frecuencia de alarmas no deseadas

- Retardo
  - Tiempo para vencer los obstáculos

- Respuesta
  - Probabilidad de comunicación precisa a las fuerzas de respuesta
  - Tiempo para comunicar
  - Probabilidad desplegarse hacia la ubicación del adversario
  - Tiempo para desplegarse
  - Efectividad de la fuerza de respuesta

Asis International. (2012). “Protection of Assets, Physical Security”.

OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD

## MODELO DE SEGURIDAD FISICA

ORGANISMO TÉCNICO DE CAPACITACIÓN

- DETERMINAR OBJETIVOS DE PPS
  - CARACTERISTICAS INSTALACION
  - DEFINICIÓN DE AMENAZA
  - IDENTIFICACION DE OBJETIVOS
- DISEÑO DE PPS
  - SISTEMAS DE PP
    - DETECTAR
      - SENSORES EXTERIORES
      - SENSORES INTERIORES
      - EVALUACION DE ALARMAS
      - COMUNICACIÓN DE ALARMAS Y MONITOREO
      - CONTROL DE ACCESO
    - DEMORAR
      - ACCESO DEMORADO
    - RESPUESTA
      - FUERZA DE RESPUESTA
      - COMUNICACIÓN CON FUERZA DE RESPUESTA
- ANALISIS DE DISEÑO DE PPS
  - ANALISIS Y EVALUACION
  - EVALUACION DE RIESGOS

OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD

# PREMISAS ADICIONALES

- Si el impacto es inaceptable, se deben tomar medidas para reducir el riesgo.
- El retardo sin detección es sólo disuasión.
- La detección es más efectiva mientras más lejos está del activo, y el retardo es más efectivo más cerca del activo (asumiendo que hay detección oportuna).
- La detección sin evaluación no es efectiva.

---

Asis International. (2012). “Protection of Assets, Physical Security”.

OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD

# EL CONCEPTO DE SEGURIDAD FISICA

"Es el diseño de contramedidas necesarias en una instalación una vez analizados los riesgos
Los riesgos, los activos de valor y las vulnerabilidades"

---

Asis International. (2012). "Protection of Assets, Physical Security".

# Contramedidas en un PPS

- SISTEMAS DE DETECCION:

  - Sensores
  - Video vigilancia
  - Comunicación de alarmas
  - Iluminación
  - Control de accesos.

# Contramedidas

## disuación

- Prevención del delito a través del diseño ambiental

## detección

- Sensores
- Video vigilancia
- Iluminación
- Comunicación de alarmas y sisualización
- Control de acceso

## retardo

- Barreras de retardo

## respuesta

OTEC MSEREY

CENTRO DE ESTUDIO DE SEGURIDAD

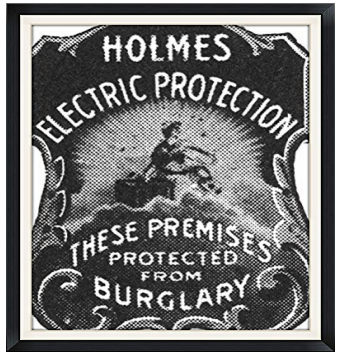
# Sabías, ¿quién y en qué año inventó las alarmas?

La primera alarma de seguridad tiene su origen en el año 1853. Su inventor fue Augustus Russell Pope de Sommerville.

Pope creo un dispositivo a base de una campanilla conectada a un circuito eléctrico en paralelo.

Este aparato se ubicaba en puertas y ventanas. Al momento de abrir una puerta o ventana, el circuito generaba por medio de la corriente eléctrica la vibración de los imanes del sistema.

Las oscilaciones electromagnéticas sacudían un martillo, el cual golpeaba la campanilla y concebía la alarma sonora.




# EDWIN HOLMES FUE EL PRECURSOR DE LAS INSTALACIONES DE ALARMAS MODERNAS.

Holmes en 1857 le compó los derechos del invento a Pope y fundó la empresa “Holmes Electric Protection Company”.

Con una estrategia publicitaria potente instauró la alarma antirrobo asociada a la telegrafía. Sistema novedoso de gran interés en esa época.

Holmes aprovecho el cableado telegráfico para trasmitir la señal de las alarmas de sus clientes hasta su oficina central.

Más adelante, el hijo de Edwin Holmes hizo la jugada maestra. Obtuvo la exclusividad de uso de la red telefónica de Nueva York para trasmitir sus sistemas de alarma por esa red cableada. El éxito fue total.

# EL TELEGRAFISTA EDWARD A. CALAHAN EN 1867 CREA LA OFICINA CENTRAL DE EMERGENCIAS.

Su invento consistía en colocar una caja de alarma con una campanilla en cada casa de un sector residencial conectadas entre sí. De este modo, se podía determinar en qué lugar se estaba produciendo un robo.

Calahan quiso ir más allá. Entendió que el sistema de alarma aparte de emitir la alerta sonora debía tener asistencia en terreno, para lo cual creo la central de llamada de emergencia.

El servicio consistía en dividir la ciudad de New York en distritos. Cada distrito sería atendido por chicos de recados, quienes acudirían al lugar de la llamada de emergencia a prestar ayuda en el menor tiempo posible. Calahan fue uno de los fundadores de la empresa ADT (American District Telegraph) en el año 1871.

# Sensores: Definiciones básicas

**Detección:** “El acto de descubrir un intento (exitoso o no) de intrusión a un perímetro protegido (Como escalar un cerco, abrir una ventana cerrada o ingresar a un área sin autorización)”.

**Sistema de detección de intrusos:** “Un sistema que utiliza uno o varios sensores para detectar una intrusión de seguridad inminente o real e iniciar una alarma o notificación del evento.”

Facilities physical security measures guideline, (2009) Asis internacional

# Sensores: Definiciones básicas

**Alarma:** “Es el mecanismo que reacciona ante un evento programado, alertando éste de manera sonora, visual o mediante la combinación de ambos, y manteniendo su condición de alerta hasta que el evento haya sido reconocido.” )”.

**Los Sensores**: “Son los encargados de controlar e informar de las variaciones que se producen en su campo de acción y determinar si están en su margen de tolerancia o constituyen una indicación exacta de que se han modificado las condiciones de trabajo normal.”

Facilities physical security measures guideline, (2009) Asis internacional

# Cómo evaluar el desempeño del sistema

- Probabilidad de detección (PD)
- Tasa de alarmas no deseadas
- Vulnerabilidad a la anulación

“protección of assets, physical security guideline, (2012) Asis internacional

# Probabilidad de detección depende de algunos factores tales como:

- **Características del intruso o el objeto a detectar**

  Velocidad (Ejemplo: 0.025 m/sec - 10.0 m/sec)
  Orientación (Ejemplo: erguido, gateando, rodando)
  Tamaño/Masa (Ejemplo: mínimo 30 kgs.)
  Preparación, herramientas y disponibilidad del intruso (o fugitivo)

- **Efectos adversos del clima (Ambiente - mantención)**

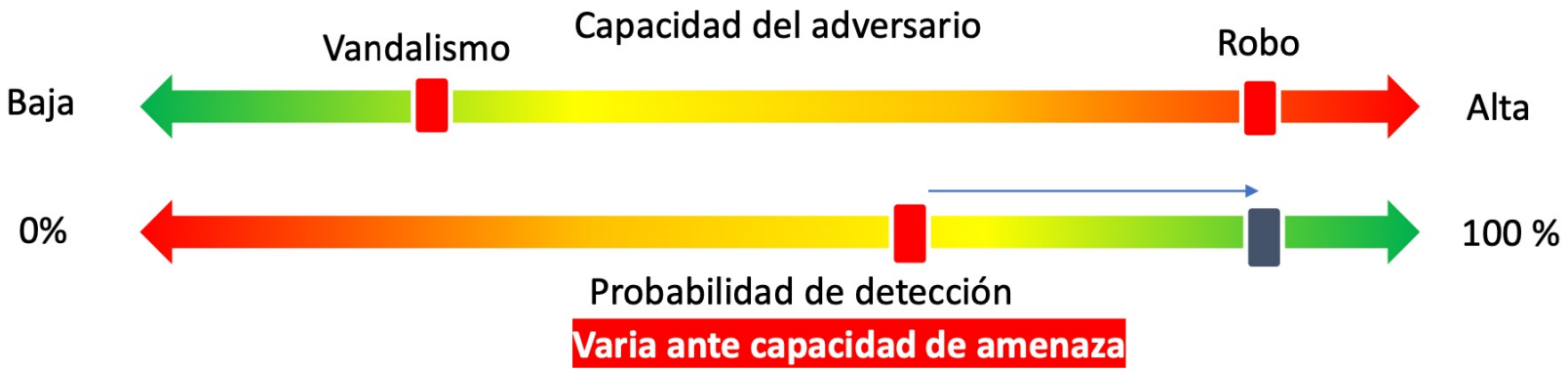
  Limitaciones inherentes de cada tecnología de sensor (Ejemplo: video en condiciones de lluvia o niebla)

- **Selección e Instalación del sensor (harward – instalación – sensibilidad**

  Sensor apropiado para el propósito, sitio y sus particularidades (Ejemplo: muro)
  Topografía del sitio (Ejemplo: Línea de vista para microondas)

# Criterios de especificación

**Amenaza de base de diseño**: "El adversario Baja contra el cual el elemento debe ser protegido" (**Protection of Assets, Physical Security" (2012)** ).




**Ejemplo 1:**

"El sistema de detección de intrusión perimetral será capaz de detectar a una persona, con un peso de 35 kilos o más, cruzando la zona de detección ya sea caminando, arrastrándose, saltando, corriendo o balanceándose, a velocidades entre 0,15 a 5 metros por segundo, o trepando la valla en cualquier punto de la zona de detección, con una probabilidad de detección del 90% y de confianza del 95%."

**Ejemplo 2:**

"detección exitosa que debe ocurrir la mayor parte del tiempo"

**Asis International. (2012). "Protection of Assets, Physical Security".**

# Alarmas no deseadas (FAR/NAR)

OTEC MSEREY
CENTRO DE ESTUDIO DE SEGURIDAD

- Alarma no deseada: “Cualquier alarma que no ha sido causada por una intrusión”

- Tasa de alarmas no deseadas (NAR) “Establece el número de alarmas no deseadas durante un tiempo determinado.

**IMPORTANTE**


“Sin la evaluación, la detcción es incompleta”

“protección of assets, physical security guideline, (2012) Asis internacional

# LAS FALSAS ALARMAS

OTEC MSEREY
CENTRO DE ESTUDIO DE SEGURIDAD

***"Las falsas alarmas son un INCIDENTE DE SEGURIDAD que nadie desea y se debe trabajar para que éstas se reduzcan."***

***Lamentablemente su número está aumentando*** *tanto en la cifra global de las llamadas recibidas, que son muchísimas, tanto como las que cumplen la condición de confirmadas y tienen que comunicarse a las Fuerzas y Cuerpos de Seguridad".*

**Las CRA verifican como falsas el 99,3% de las alarmas que reciben**

*Las empresas que la desarrollan de forma independiente deben conformar un* ***binomio sincronizado*** *que funcione como un reloj buscando el mismo fin: aportar a los clientes comunes una seguridad conjunta eficiente.* ***Por tanto, las CRA no pueden desempeñar adecuadamente su trabajo si los instaladores no desempeñan adecuadamente el suyo y viceversa".***

# LAS FALSAS ALARMAS

OTEC MSEREY
CENTRO DE ESTUDIO DE SEGURIDAD

- **El 92% de las veces que los servicios policiales acuden al aviso de una alarma, su presencia es innecesaria.**

- **El 70% de las falsas alarmas las provocan los usuarios, ¿qué soluciones hay?**

- *El **problema se concentra en aquellos usuarios que propician reiteración de falsas alarmas** y además la producen sin inmutarse y sin preocuparles sus consecuencias. Podíamos explicarlo con el 'efecto Pareto', una minoría de los usuarios producen la mayor parte del problema".*

OTEC MSEREY
CENTRO DE ESTUDIO DE SEGURIDAD

# Causas

# CRITERIOS DE ESPECIFICACIÓN.

**Ejemplo 1:**

"todo el perímetro del sistema de detección de intrusión no promedie más de una falsa alarma por semana por zona, manteniendo una PD de 0.9”.

**Ejemplo 2:**

“una medida de FAR y NAR superior se puede aceptar si no empeora el sistema”

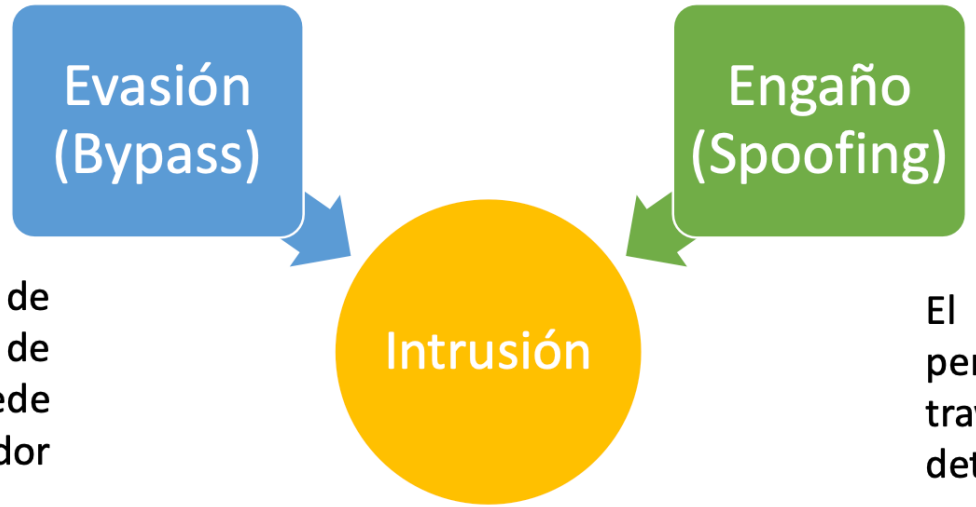
Con valores más específicos para la tasa de falsa alarma, es más fácil decidir cuándo reportar un sensor al personal de mantenimiento." (**Protection of Assets, Physical Security” (2012)** ).

**IMPORTANTE**

Es muy importante que se detecten las causa de las alarmas no deseadas y se resuelvan para poder reducir vulnerabilidades a nivel de evaluación de alarmas y otras consecuencias negativas. El exceso de falsas alarmas representa una vulnerabilidad significativa ya que crea hábitos en los operadores de reconocer una alarma como falsa cuando puede ser una intrusión real, y que no se pueda evitar el robo. En algunos países las falsas alarmas en las que acude la policía pueden generar multas.

# Vulneración a la anulación

Todos los sensores pueden ser burlados. El objetivo del diseñador de un PPS es hacer que el sistema sea muy difícil de anular. Hay dos formas para anular o burlar el sistema:




Debido a que todos los sensores de intrusión tienen una zona finita de detección, cualquier sensor puede ser burlado moviéndose alrededor de su volumen de detección.

El engaño es una técnica que permite llegar a destino pasando a través de la zona normal de detección sin generar una alarma.

**Asis International. (2012). "Protection of Assets, Physical Security".**

# Métodos de anulación

"La tecnología de cada sensor funcionará dentro de los límites de las leyes de la física, y las interacciones entre el hardware del sensor y el entorno físico también son parte de la evaluación, en conjunto con la instalación, el mantenimiento y los procedimientos operativos adecuados, así como una comprensión de la amenaza esperada".

**Garcia, M. (2005). Vulnerability Assessment of Physical Protection Systems.**


- Salto
- Gateo
- Túnel
- Puente

- Caminar lentamente
- Arrastrarse lentamente
- Obstruir el campo de detección

**IMPORTANTE**

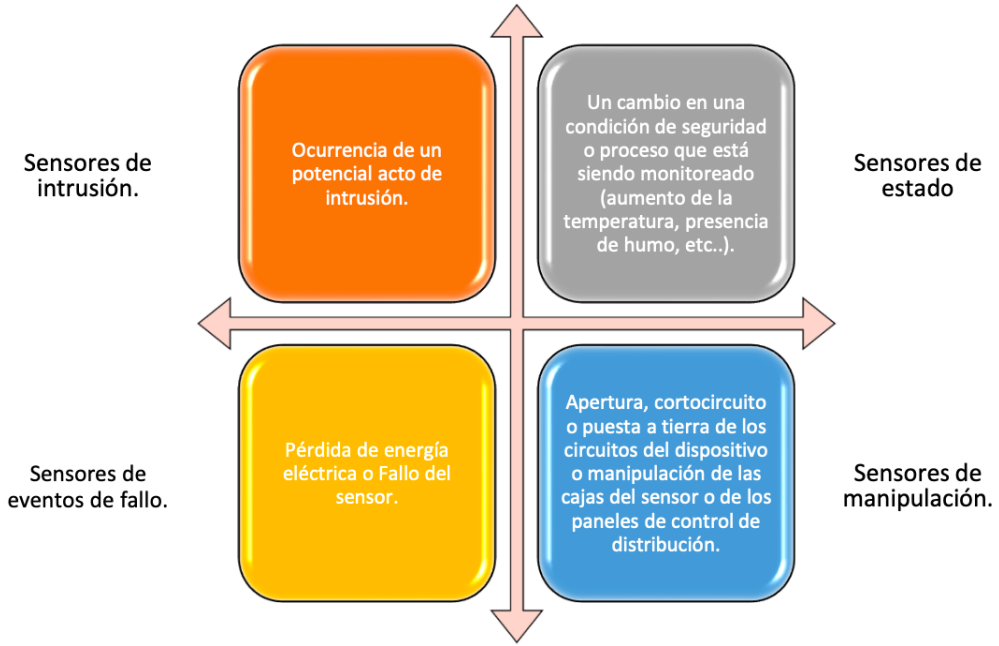
Un método común de anulación para todas las tecnologías es el sabotaje o manipulación (tampering). Este método consiste en atacar uno o varios elementos del sistema con la finalidad de anularlo.

Entre los elementos más comúnmente más atacados están el suministro eléctrico, comunicación y los sensores en sí. Este tipo de ataques se pueden reducir a través de un diseño, instalación, configuración y mantenimiento adecuados.

# Condición de iniciación y funcionamiento

**Iniciación:**

En un SPF deberían incluirse sensores de todo tipo para iniciar una alarma bajo cualquiera de las siguientes condiciones:




**Funcionamiento:**

- Sensores interiores: rango de temperatura entre 32°F a 120°F (0°C a 49°C).
- Sensores exteriores o en estructuras sin calefacción: rango de temperatura entre -30°F a 150°F (-34°C a 66°C).
- Todas las unidades deben ser capaces de funcionar a 90°F (32°C) con un 95% de humedad relativa.

**Asis International. (2012). "Protection of Assets, Physical Security".**

# Estándares, normas y especificaciones.

Estándares:

UL: 681, 1076, 1641.

ASTM: STP729 Building Security, Stroik J (1.981) Normas:

• NFPA 72
Especificaciones y otros documentos:

WA-450C/GEN, GSA.

Intrusion Detection System Handbook, Sandia Laboratories, Albuquerque, NM.

**Asis International. (2012). “Protection of Assets, Physical Security”.**

# Dispositivos

**Posición**

**Movimiento**

- Microondas
- Infrarrojos
- Doble tecnología
- Ultrasónicos
- Haz de luz

**Sonido**

**Vibración**

**Calor**

**Temperatura**

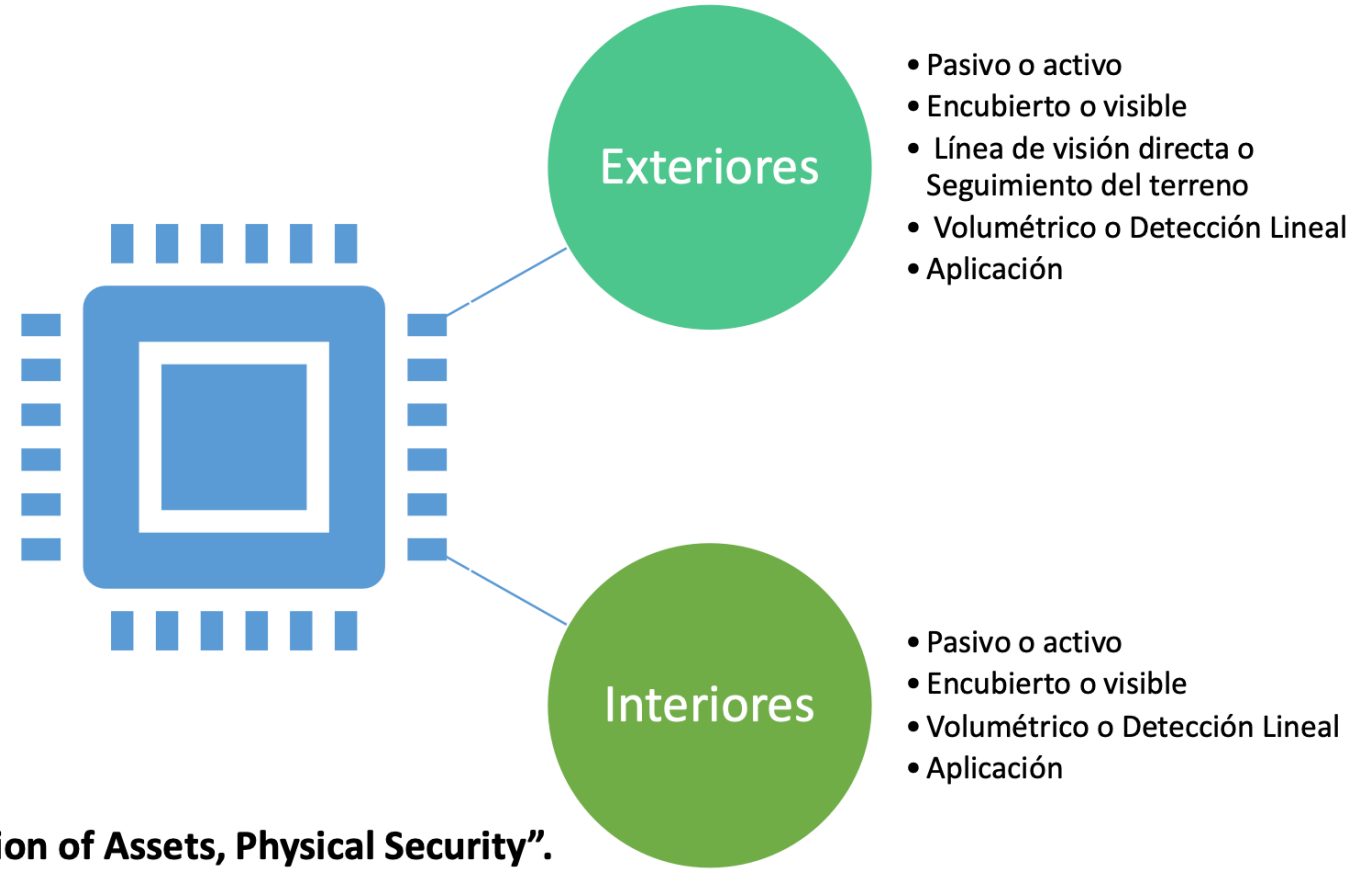
**Capacitancia**

**Impacto**

**Ruptura de vidrio**

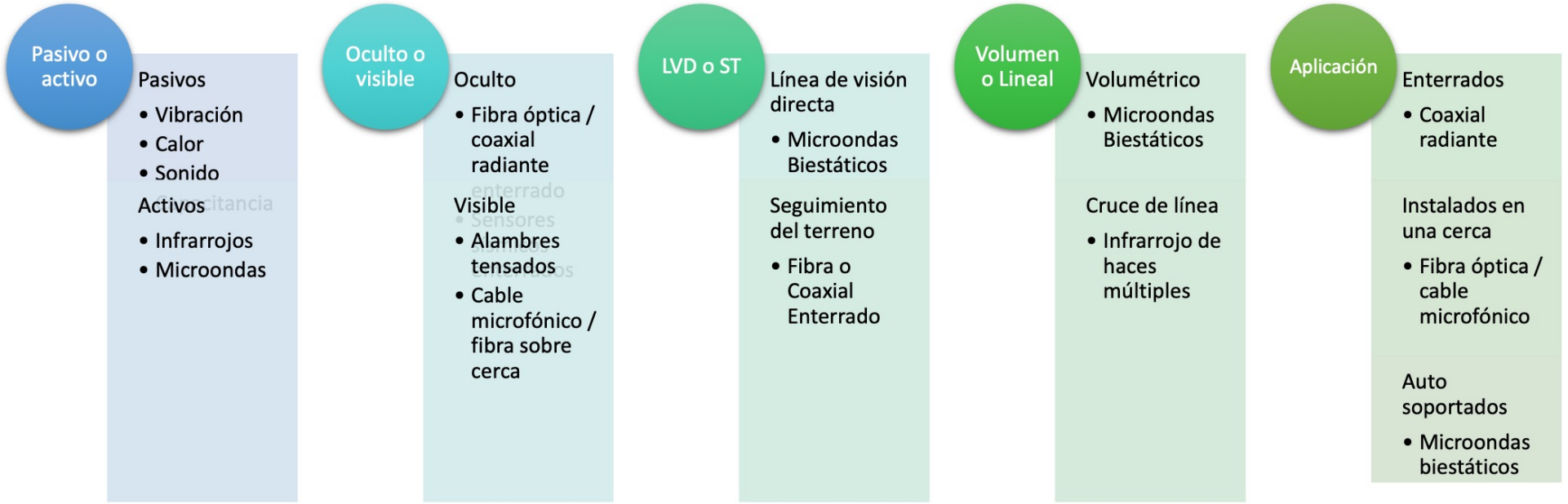
**Pánico / coacción**

# Tipos de sensores




**Asis International. (2012). "Protection of Assets, Physical Security".**

# Sensores exteriores




**Asis International. (2012). "Protection of Assets, Physical Security".**

# Clasificación

| | Passive or Active Detection | Covert (C) or Visible (V) | Line of Sight (LOS) or Terrain Following TF | Volumetric (V) or Line (L) |
|---|---|---|---|---|
| **Buried Line** | | | | |
| Seismic Pressure | P | C | TF | L |
| Magnetic Field | P | C | TF | VOL |
| Ported Coax | A | C | TF | VOL |
| Fiber Optic Cables | P | C | TF | L |
| **Fence-Associated** | | | | |
| Fence Disturbance | P | V | TF | L |
| Sensor Fence | P | V | TF | L |
| Electric Field | A | V | TF | VOL |
| **Freestanding** | | | | |
| Active Infrared | A | V | LOS | L/VOL* |
| Passive Infrared | P | V | LOS | VOL |
| Bistatic Microwave | A | V | LOS | VOL |
| Dual Technology | A | V | LOS | VOL |
| Video Motion | P | C | LOS | VOL |

# Sensores interiores

**Pasivo o activo**

Pasivos
- Vibración
- Calor
- Sonido
- Capacitancia

Activos
- Infrarrojos
- Microondas

**Ocultos o visibles**

Ocultos
- Fibra óptica / coaxial radiante enterrado
- Sensores sísmicos enterrados

Visibles
- Alambres tensados
- Cable microfónico / fibra sobre cerca

**Volumétrico o Detección Lineal**

Volumétrico
- Microondas Biestáticos

Cruce de línea
- Infrarrojo de haces múltiples

**Aplicación**

Sensores de penetración de perímetro.
- Sensores sísmicos

Sensores de movimiento interior.
- Sensores pasivos infrarrojos
- Sensores doble tecnología

Sensores de proximidad.
- Sensores de capacitancia

# Clasificación

| | Passive or Active | Covert or Visible | Volumetric or Line |
|---|---|---|---|
| **Boundary Penetration Sensors** | | | |
| Electromechanical | P | C | L |
| Infrared | B* | V | L |
| Vibration | P | C | L |
| Capacitance | P | C | L |
| Fiber Optic | P | E* | L |
| **Interior Motion Sensors** | | | |
| Microwave | A | V | V |
| Infrared | P | V | V |
| **Proximity Sensors** | | | |
| Capacitance | P | C | L |
| Pressure | P | C | L |
| Fiber Optic | P | E* | L |

B* - Both active and passive types exist

# Transmisión, monitoreo y notificación.

- Las señales de alarma se pueden transmitir a los sistemas de monitoreo de alarma y al personal.
- Se pueden transmitir por cable o de forma inalámbrica, y por zona o por un punto de alarma individual.
- Ser capaz de identificar un punto de alarma en particular puede reducir el tiempo de respuesta del oficial de seguridad y facilitar la identificación de puntos de alarma que funcionan mal.
- Las transmisiones de alarma, los medios / dispositivos de monitoreo y notificación deben ser supervisados para detectar mejor los casos de manipulación o intercepción.
- Se deben realizar pruebas periódicas para garantizar la precisión y la puntualidad de la información transmitida.
- El monitoreo de alarmas, realizado internamente (propietario) o por contrato, puede hacer que se notifique al propietario del sistema por varios métodos, incluidos teléfono, correo electrónico y buscapersonas.
- Se debe desarrollar una lista de todas las personas que se notificarán y sus números de teléfono asociados (y la información de contacto alternativa).

**Mejor práctica: Un sensor por zona**

**Comunicación y energía**

**Supervisión de fin de línea**

**Facilities Physical Security Measures Guideline,** (2009), ASIS International.

**IMPORTANTE**

El listado de personal y números a ser notificado se debe actualizar trimestralmente o cuando se tenga notificación de cambios de personas o números.

# Instalación, mantenimiento y reparación.

- **Ingeniería e instalación**. son esenciales para un sistema de alarma que funcione correctamente. Incluso si todos los dispositivos, paneles y anunciadores son de buena calidad, el sistema fallará sin una ingeniería de diseño adecuada, si los componentes seleccionados no están instalados correctamente o no son los componentes correctos para la aplicación.

Contrato + SLA

- **Puesta en marcha:** es el proceso de probar cada punto de alarma y cada función automática de un nuevo sistema.

- **Auditoría:** proceso continuo de prueba y documentación de las operaciones de un sistema de seguridad para garantizar que todas las partes funcionen correctamente.

- **Mantenimiento:** los sistemas de alarma requieren un mantenimiento regular, que puede proporcionar el personal de la instalación (como un especialista en sistemas de seguridad interno) o los proveedores de sistemas.

Contrato + SLA

- **Reparación:** Las reparaciones se pueden manejar de la misma manera que los problemas de mantenimiento.

**Facilities Physical Security Measures Guideline,** (2009), ASIS International.

**IMPORTANTE**

- El proceso de ingeniería de diseño incluye los requerimientos de selección, ubicación, medidas de respaldo de comunicación y energía, instalación, configuración, prueba y procedimientos de utilización, monitoreo y respuesta.
- En el caso de sistemas de alarmas monitoreados en central de monitoreo, el sistema debe contar con al menos 2 sistemas de comunicación distintos.

Sistema de Seguridad Electrónica es aquel que permite expandir de manera significativa los sentidos del hombre, es decir, el tacto, visión, oído o las capacidades de aviso, memoria y raciocinio del ser humano, a limites insospechados, ayudando de esta manera a prevenir accidentes o la manifestación de otro tipo de riesgo como son los delitos de robos u otros.

## ¿QUE ES UN SISTEMA DE SEGURIDAD ELECTRÓNICA?