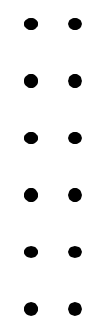
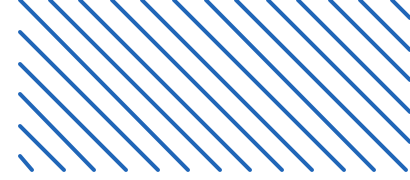


Oficial de Protección Certificado Certified Protection Officer



CPO©



Título de la Unidad V

PROTECCION DE PROPIEDADES



CPO©



INSTRUCTOR

CPO CPOI CSSM

• RESUMEN

EXPERTO ASESOR

MARCELO SEREY GONZALEZ

Subprefecto (R) Policía de Investigaciones de Chile

Licenciado en Investigación Criminalística PDI.

Ingeniero Prevencion de Riesgos UTFM.

Asesor y capacitador en Seguridad Privada.

Presidente Capítulo Chile IFPO Internacional.

Director "Centro de Estudios de Seguridad MSEREY"

CERTIFICACIONES INTERNACIONALES

Oficial Certificado de Proteccion

Instructor Certificado de Oficiales de Protección

IFPO - Fundacion Internacional de oficiales de Protección.



INTERNATIONAL
FOUNDATION FOR
PROTECTION OFFICERS
KNOWLEDGE TO PROTECT

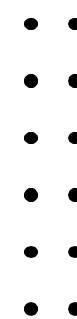


Acuerdos de aprendizaje

- Respeto



CPO©



PROTECCION DE PROPIEDADES

Manual CPO.



CPO®

INTRODUCCIÓN

¿QUE ES LA PROTECCIÓN FISICA?

ASIS Internacional a definido Seguridad física como :

La parte de la seguridad relacionada con los medidas físicas destinadas a proteger a las personas; para evitar el acceso no autorizado a los equipos, instalaciones, materiales y documentos; y para protegerlos contra un incidente de seguridad.

La seguridad física de instalaciones la vamos a definir como el diseño de contramedidas implementadas una vez analizados los activos, las vulnerabilidades y a amenazas.

La regla de oro de ASIS Internacional, es que la brújula que orienta a la administración en la implementación de las medidas de mitigación debe ser el nivel de riesgo existente.



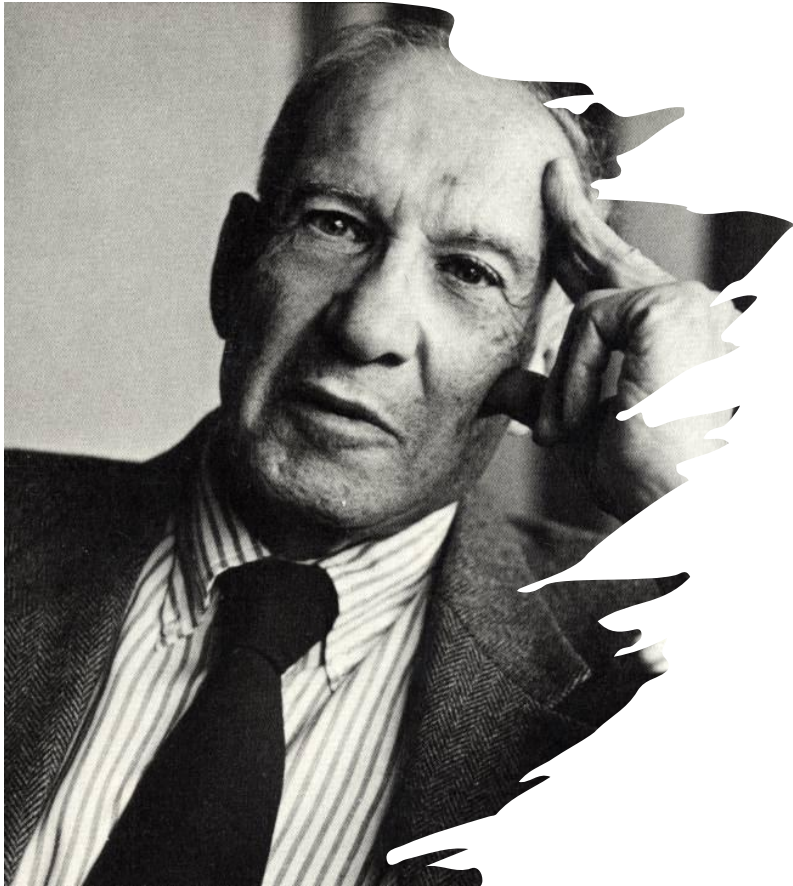
OBJETIVO DEL CAPÍTULO

OBJETIVO GENERAL DE LA UNIDAD:

Explicar los diversos elementos de la planificación de seguridad física y por qué son importantes, realizar un tour de instalaciones para explicar a la clase las medidas de seguridad física presentes.



PASOS BÁSICOS EN LA PROTECCIÓN FÍSICA.



"El primer deber del negocio es sobrevivir y el principio guía de la economía comercial no es la maximización de las utilidades, sino el evitar las pérdidas."

Peter Drucker

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.

$$R = H \times V - M$$

Diagram illustrating the Risk Equation: $R = H \times V - M$. The variables are labeled with arrows:

- R (Risk) is labeled with an arrow pointing to it from the word "risk".
- H (Hazards) is labeled with an arrow pointing to it from the word "hazards".
- V (Vulnerability) is labeled with an arrow pointing to it from the word "vulnerability".
- M (Mitigation) is labeled with an arrow pointing to it from the word "mitigation".

PREMISA BASE

Amenazas

"Causa potencial de un incidente indeseado, que puede dar como resultado daños a las personas, a los activos, a un sistema o una organización, al entorno, o a la comunidad". ANSI/ASIS PAP.1-2012.

"Una vulnerabilidad es cualquier debilidad o práctica de negocio que pueda ser explotada por un adversario o que hace a un activo susceptible a daños causados por amenazas naturales o inadvertidas"
Physical Security Principles. (2015)

Vulnerabilidades

Activos

"Cualquier elemento que tenga un valor tangible o intangible para la Organización",
ANSI/ASIS/RIMS RA.1-2015.

Probabilidad / Frecuencia.

"Posibilidad de que algún hecho se produzca."
ANSI/ASIS PAP.1-2012. / ANSI/ASIS/RIMS RA.1-2015.

"Cantidad de veces que un evento dentro de un periodo acotado de tiempo".

Consecuencia / Impacto.

"Resultado de un suceso que afecta a los objetivos,"
ANSI/ASIS PAP.1-2012.

"Consecuencia evaluada de un resultado en particular".
ANSI/ASIS PAP.1-2012.

© 2018 Ali Ferrer

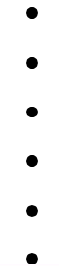
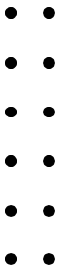
PREMISA BASE

Seguridad física:

....” Aquella parte de la seguridad que se ocupa de las medidas de seguridad diseñadas para proteger a las personas, prevenir accesos no autorizados a equipamiento, instalaciones, materiales y documentos y protegerlos ante incidentes de seguridad”

Medida de seguridad física:

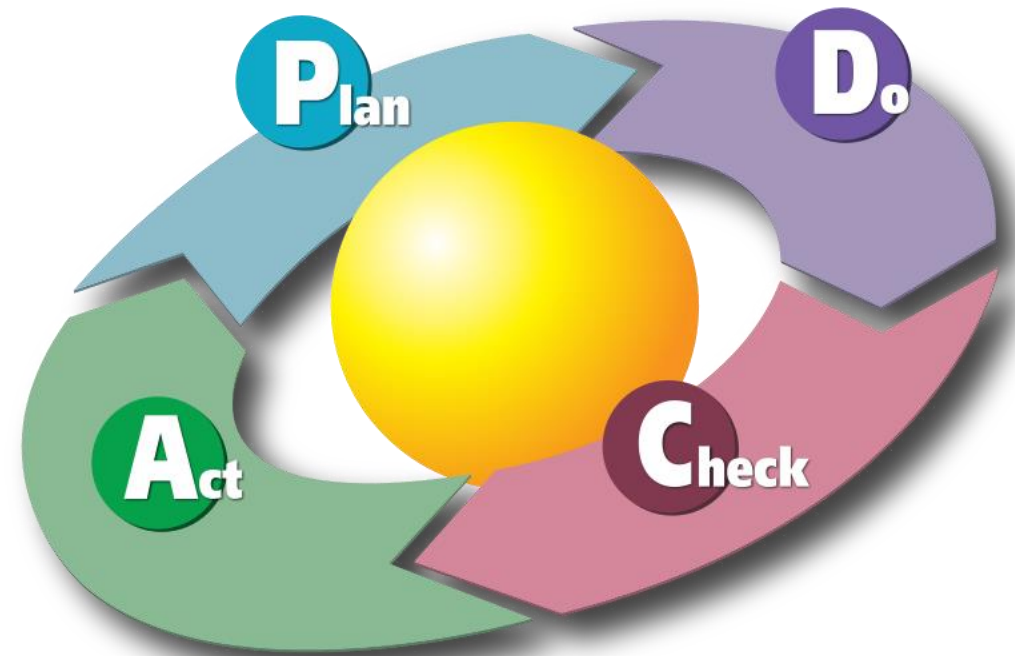
“Dispositivo, sistema o práctica de naturaleza tangible diseñada para proteger a las personas y evitar daños, pérdidas o acceso no autorizado a los activos”.



PASOS BÁSICOS EN LA PROTECCIÓN FISICA.

Existen cinco áreas principales de consideración para la protección de instalaciones:

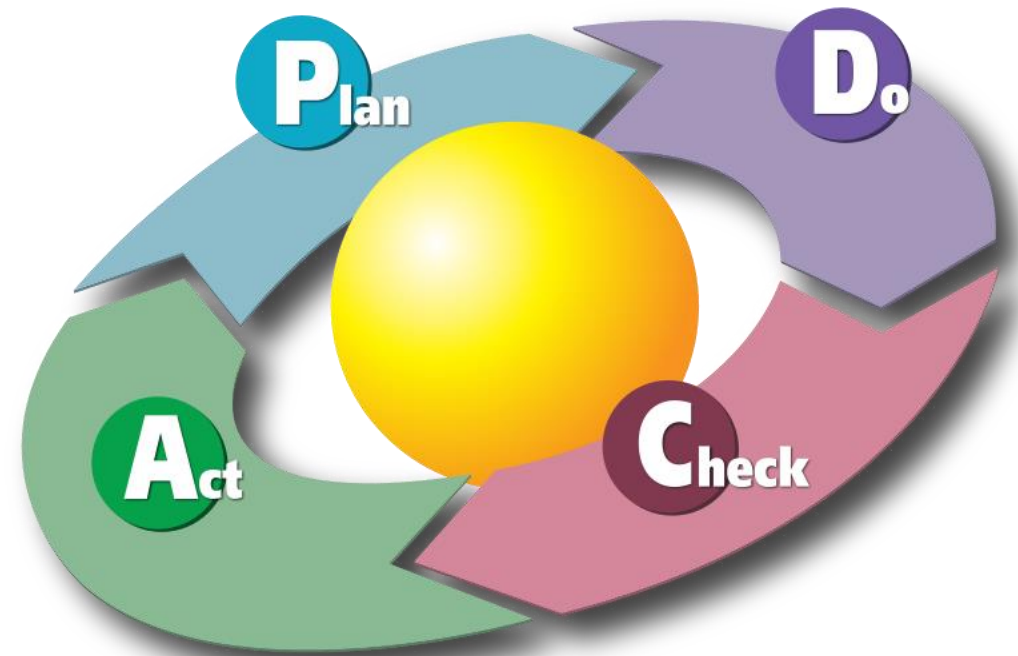
- ❖ IDENTIFICAR PELIGROS.
- ❖ EVALUACIÓN DE RIESGOS.
- ❖ SELECCIÓN DE CONTRAMEDIDAS.
- ❖ IMPLEMENTACIÓN DE CONTRAMEDIDAS.
- ❖ SUPERVISAR LA EFECTIVIDAD DEL SISTEMA.



SUPERVISIÓN DE LA EFECTIVIDAD DEL SISTEMA

Existen cinco áreas principales de consideración para la protección de instalaciones:

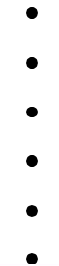
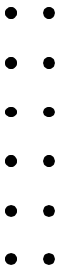
- ❖ IDENTIFICAR PELIGROS.
- ❖ EVALUACIÓN DE RIESGOS.
- ❖ SELECCIÓN DE CONTRAMEDIDAS.
- ❖ IMPLEMENTACIÓN DE CONTRAMEDIDAS.
- ❖ SUPERVISAR LA EFECTIVIDAD DEL SISTEMA.



IDENTIFICAR PELIGROS.

La identificación de peligros resulta fundamental para la planificación de un sistema de seguridad; en este contexto “Saber qué quieres proteger y que peligro o amenaza lo puede afectar, nos invita a Implementar el tipo de medida de seguridad adecuada.”

ACTIVOS: SE REFIERE A CUALQUIER ELEMENTO QUE TENGA UN VALOR TANGIBLE O INTANGIBLE PARA LA ORGANIZACIÓN”



PASOS BÁSICOS EN LA PROTECCIÓN FÍSICA.



PERSONAS. Capital humano – trabajadores, contratistas, clientes visitantes, la comunidad.



INFORMACIÓN: Constituye el capital intelectual, información propietaria desarrollada o acumulada con esfuerzo, datos confidenciales, planes).



PROPIEDADES: Constituyen el capital financiero: Muebles e inmuebles que poseen características físicas.



IMAGEN: Constituyen el capital comercial: Reputación pública frente a clientes, posicionamiento del negocio.

VALORACION DE ACTIVOS

CUALITATIVO

Se basa en establecer escalas cualitativas para evaluar y clasificar los activos de acuerdo a uno o más parámetros:

- Impacto (en caso de pérdida) sobre la operación: parada total, parcial, breve, sin parada.
- Alternabilidad: redundancia total, redundancia parcial, redundancia reducida, sin redundancia.
- Tiempo de reposición: se puede reponer rápidamente, se puede reponer en el mediano plazo.
- Costo: Muy alto, alto, medio, bajo, muy bajo.

Todos los activos se evalúan bajo los mismos parámetros y se clasifican de acuerdo al resultado, si esta información es considerada en conjunto con las amenazas y vulnerabilidades se puede establecer la prioridad para la aplicación de medidas.

VALORACION DE ACTIVOS

CUANTITATIVO

Se considera el peor escenario para cada riesgo, estimando una perdida máxima probable, con la siguiente formula:

$$K = (C_p + C_t + C_r + C_i) - I$$

Donde :

K= costo total de la pérdida.

C_p= costo de reposición.

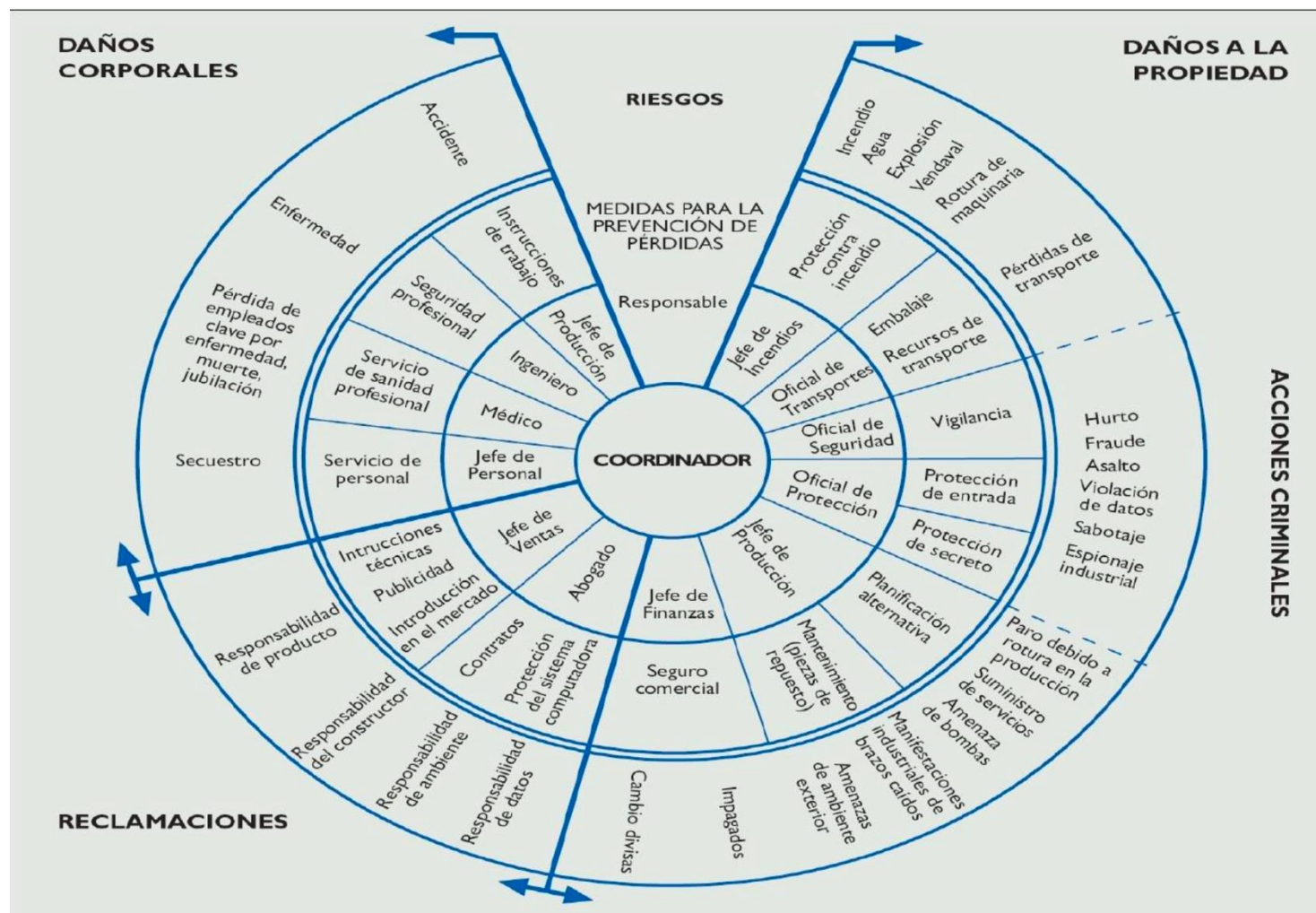
C_t= costo de sustituto temporal.

C_r= Costos relacionados (reinstalación, etc.)

C_i= Costo de ingresos perdidos

I= Indemnización o seguro disponible.

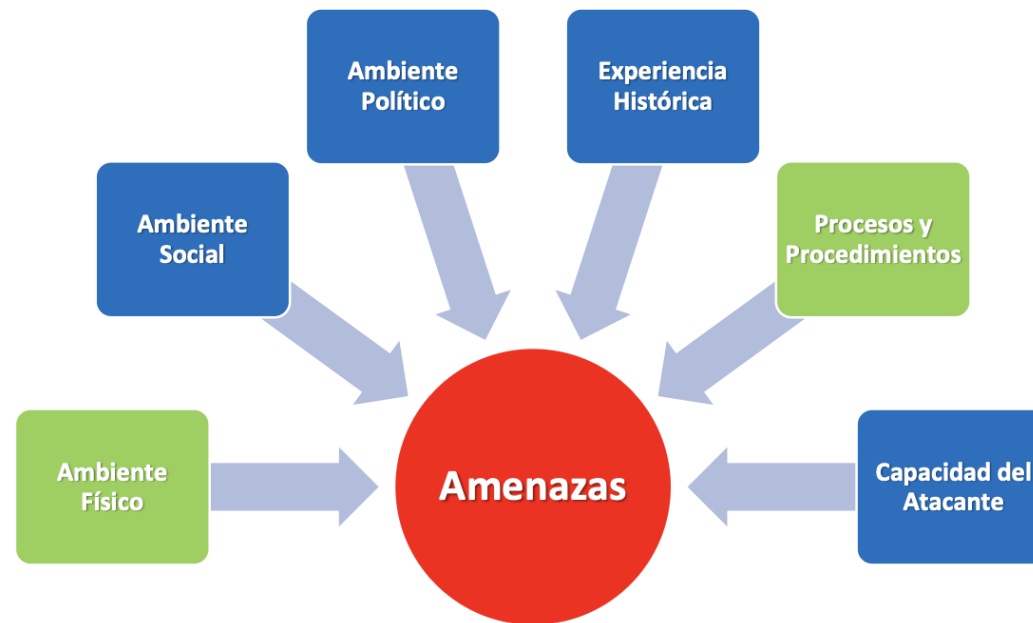
IDENTIFICAR PELIGROS.



IDENTIFICACION DE AMENAZAS

Probabilidad: Cantidad de veces que ocurre un evento dado en un número igualmente posible de resultados

Frecuencia: Cantidad de veces que ocurre un evento durante un periodo de tiempo dado.



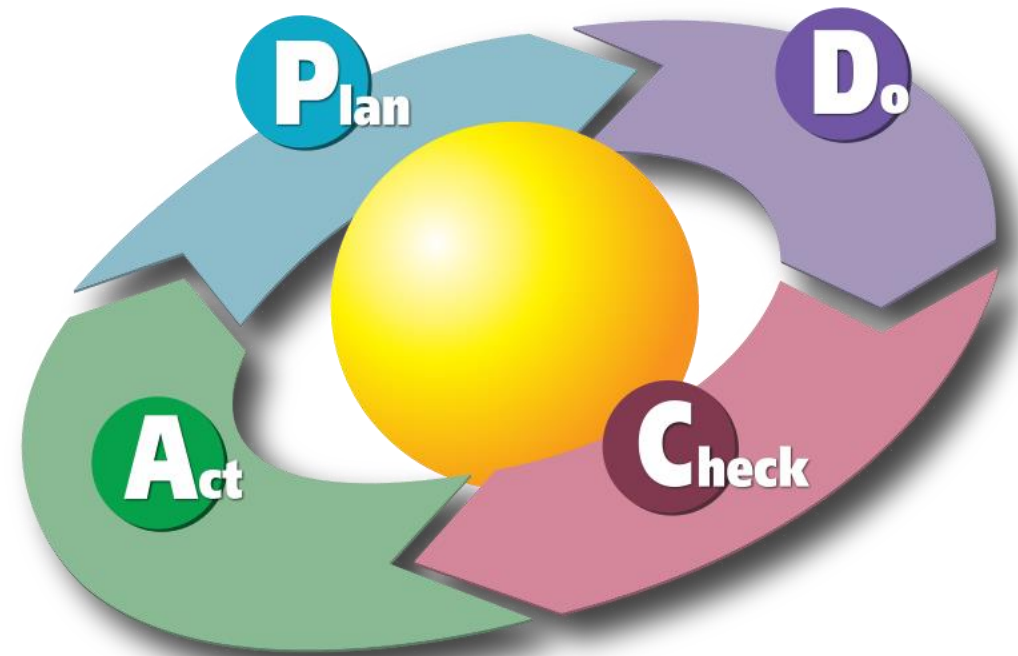
Tip:

Mientras más formas tenga de ocurrir un evento, mayor será su probabilidad de ocurrencia.

SUPERVISIÓN DE LA EFECTIVIDAD DEL SISTEMA

Existen cinco áreas principales de consideración para la protección de instalaciones:

- ❖ IDENTIFICAR PELIGROS.
- ❖ EVALUACIÓN DE RIESGOS.
- ❖ SELECCIÓN DE CONTRAMEDIDAS.
- ❖ IMPLEMENTACIÓN DE CONTRAMEDIDAS.
- ❖ SUPERVISAR LA EFECTIVIDAD DEL SISTEMA.



EVALUACIÓN DE RIESGOS

Identificado los bienes y su exposición hacia una amenaza, el siguiente paso es cuantificar la Posibilidad de que ocurra un evento de pérdida, y podemos asignar cuatro categorías a la probabilidad.

A.- CERTERO

B.- ALTAMENTE PROBABLE.

C.- MEDIANAMENTE PROBABLE

D.- IMPROBABLE.

Esta información la podemos obtener a partir del **Estudio de seguridad** en terreno, que considere entre otros: Historial de pérdidas similares, estadísticas delictivas, análisis de la estructura, historia climática del aérea; La naturaleza de la actividad de la propiedad que va a ser protegida, historial criminal de las áreas inmediatas y adyacentes; Conflictos comunitarios, etc.

EVALUACIÓN DE RIESGOS

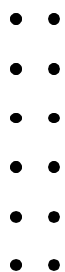
Estudio de seguridad (protección):

"Un examen físico completo de una instalación, sus sistemas y procedimientos, realizado para evaluar el nivel actual de seguridad, localizar las deficiencias y evaluar el grado de protección necesario*"

"Un examen crítico en sitio ... para determinar el estado actual de seguridad, identificar deficiencias o excesos, determinar la protección necesaria y hacer recomendaciones para mejorar la seguridad general de la operación**

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

** definición original en Risk analysis and the security survey (4th ed.). (2012). Broder, J. & Tucker, E.



EVALUACIÓN DE RIESGOS

Para completar el estudio se debe valorar el impacto de que ocurra una pérdida.

Evaluación de riesgos de seguridad:

"Es el proceso de evaluar los riesgos relacionados con la seguridad, provenientes de amenazas internas y externas a una instalación, sus activos o personal".

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

IMPACTO O CONSECUENCIAS:

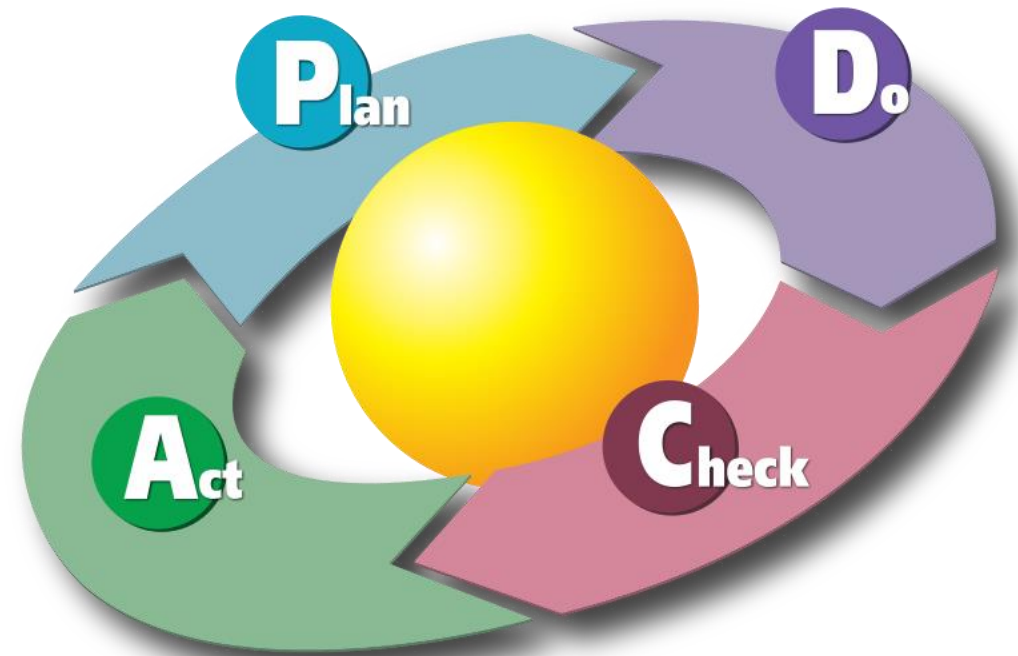
- Resultado de un suceso que afecta a los objetivos de la organización de manera directa o indirecta.
- Es la consecuencia de un resultado en particular.

- I. Muy serio
- II. Serio
- III. Moderadamente serio.
- IV. Sin importancia.

SUPERVISIÓN DE LA EFECTIVIDAD DEL SISTEMA

Existen cinco áreas principales de consideración para la protección de instalaciones:

- ❖ IDENTIFICAR PELIGROS.
- ❖ EVALUACIÓN DE RIESGOS.
- ❖ SELECCIÓN DE CONTRAMEDIDAS.
- ❖ IMPLEMENTACIÓN DE CONTRAMEDIDAS.
- ❖ SUPERVISAR LA EFECTIVIDAD DEL SISTEMA.

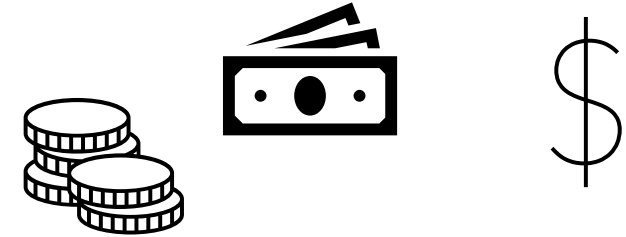


SELECCIÓN DE CONTRAMEDIDAS

Personal: Consultoría, administración, oficiales.

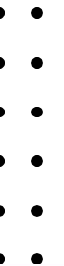
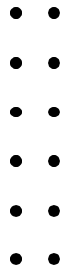
Electromecánica: Cerraduras, sistemas de seguridad, iluminación.

Modificación del comportamiento: Políticas, procedimientos, capacitación, concienciación.



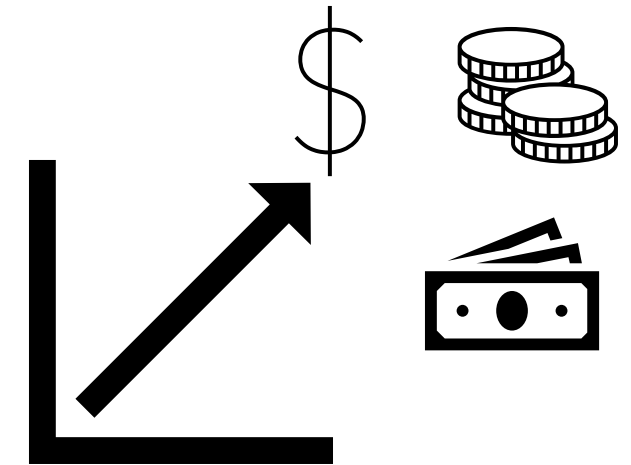
Jerarquía de
soluciones de
seguridad en relación a
su costo

Para decidir el nivel de protección necesario, podemos nuevamente usar la matriz MOR



SELECCIÓN DE CONTRAMEDIDAS

	CERTERO	ALTAMENTE PROBABLE	MODERADA- MENTE PROBABLE	IMPRO- BABLE
MUY SERIO	1	1	2	3
SERIO	1	2	3	4
MODERADA-MENTE SERIO	2	3	4	5
POCO IMPORTANTE	3	4	5	5

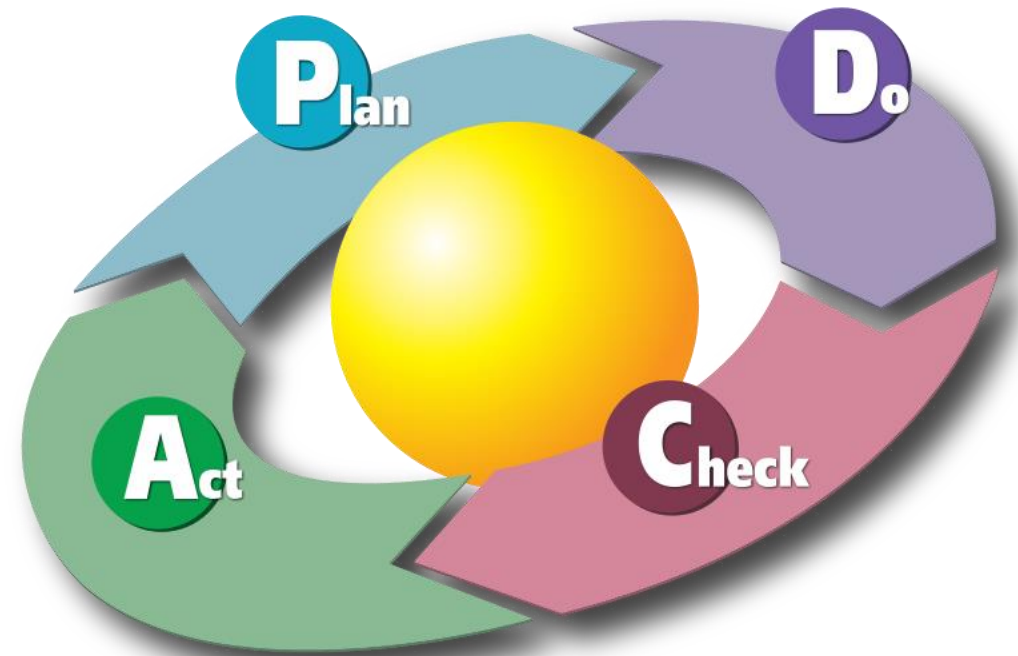


1. Critico
2. Serio
3. Moderado
4. Menor
5. insignificante

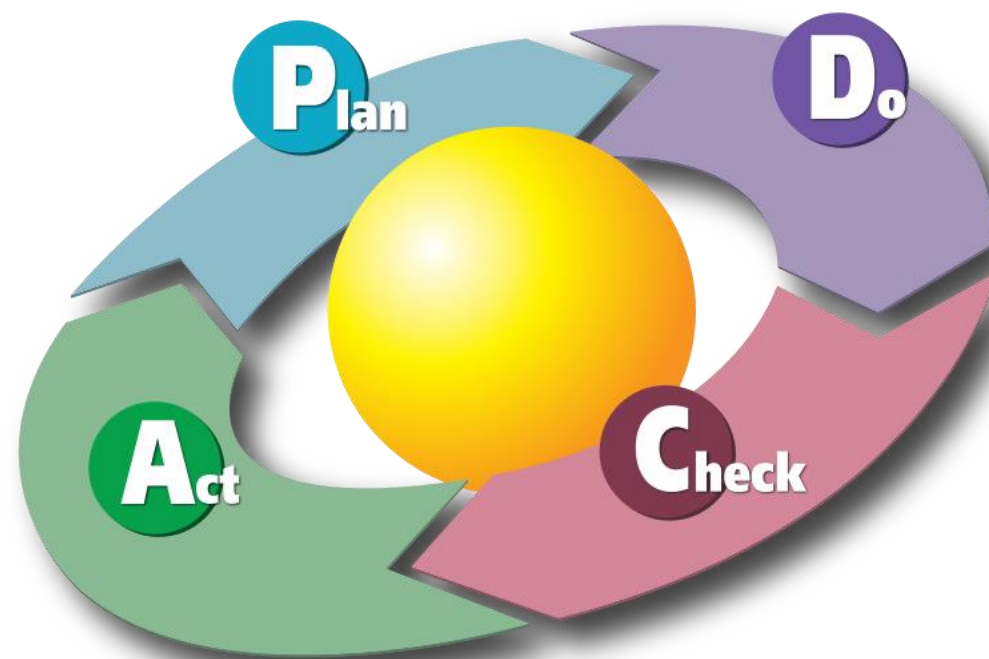
SUPERVISIÓN DE LA EFECTIVIDAD DEL SISTEMA

Existen cinco áreas principales de consideración para la protección de instalaciones:

- ❖ IDENTIFICAR PELIGROS.
- ❖ EVALUACIÓN DE RIESGOS.
- ❖ SELECCIÓN DE CONTRAMEDIDAS.
- ❖ IMPLEMENTACIÓN DE CONTRAMEDIDAS
- ❖ SUPERVISAR LA EFECTIVIDAD DEL SISTEMA.



SUPERVISIÓN DE LA EFECTIVIDAD DEL SISTEMA



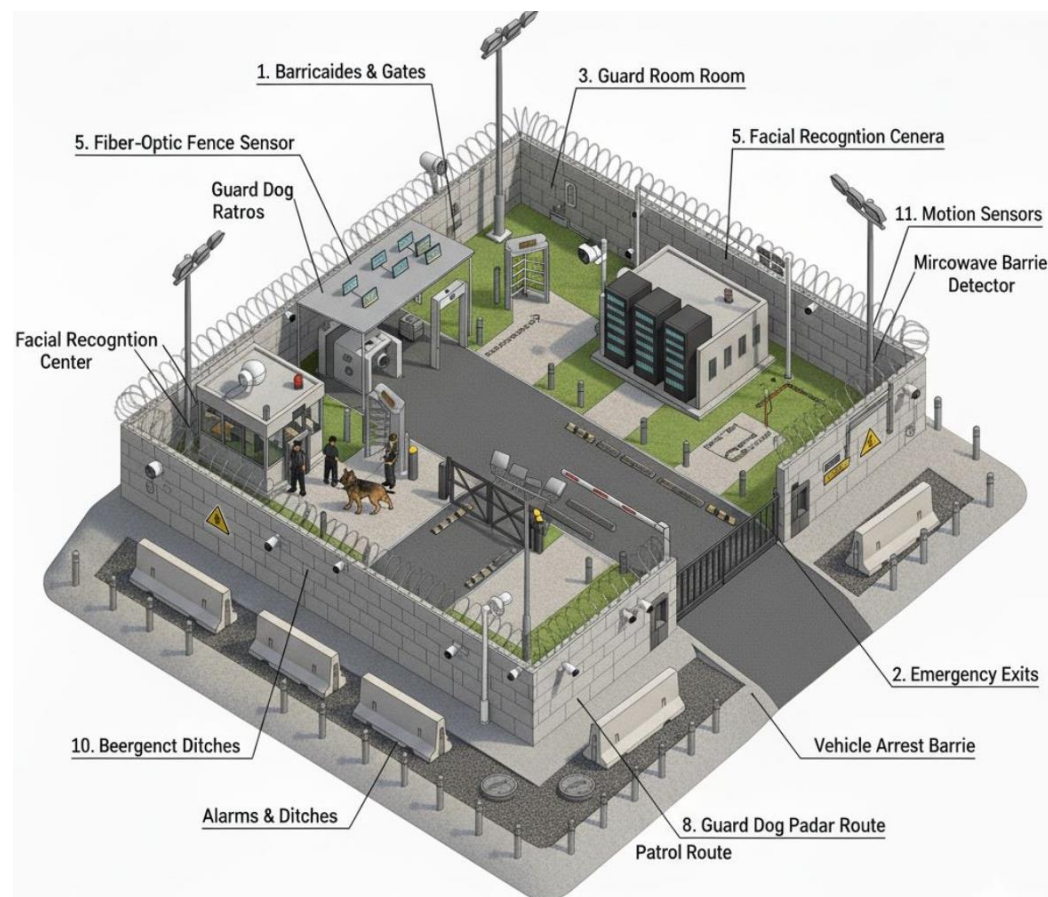
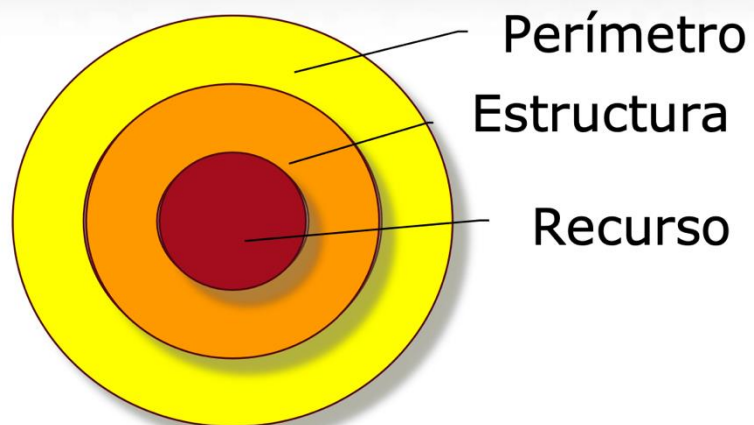
SUPERVISIÓN DE LA EFECTIVIDAD DEL SISTEMA

CARACTERÍSTICAS DE DISEÑO PARA UN
SISTEMA DE PROTECCION FISICA

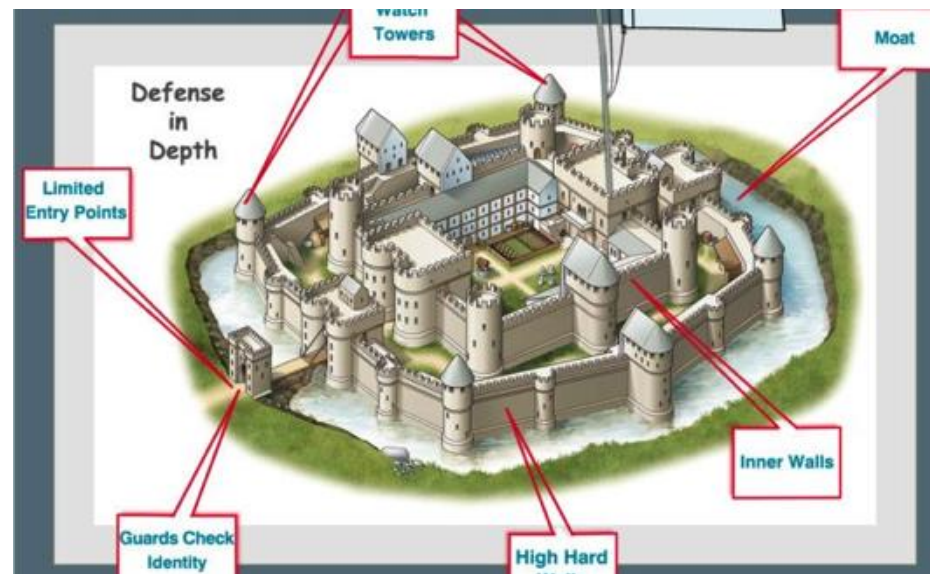


DEFENSA EN PROFUNDIDAD

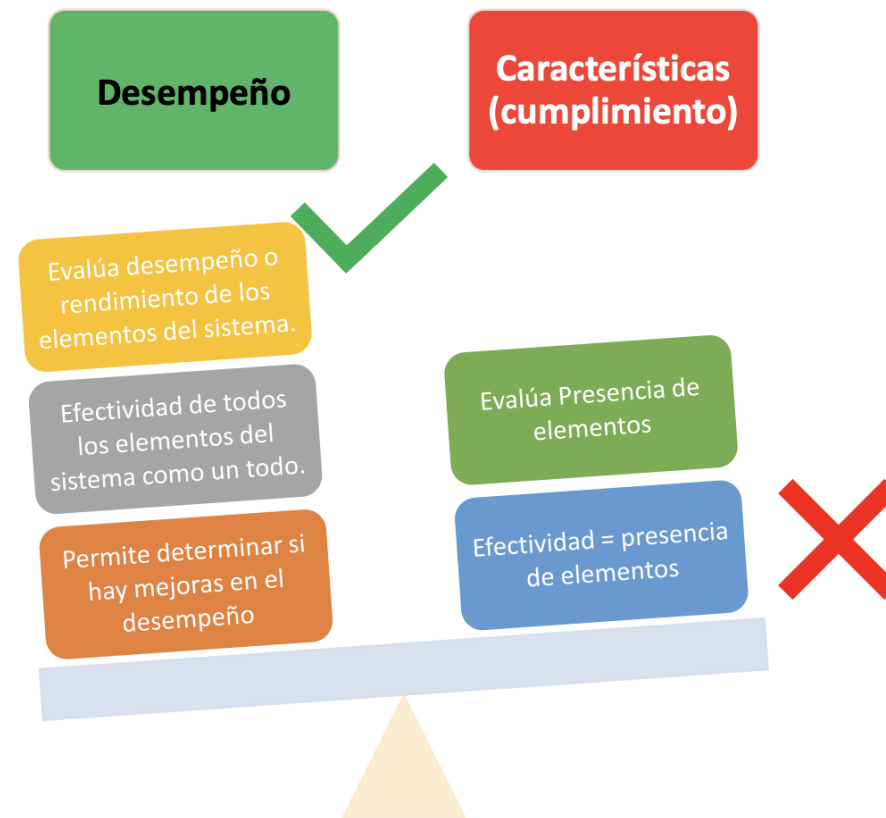
Defensa en profundidad; creando círculos concéntricos de contramedidas en el perímetro, estructura y recursos a proteger.



DEFENSA EN PROFUNDIDAD

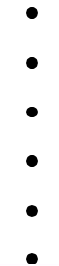
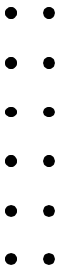


PROTECCION BALANCEADA



MEDIDAS DE SEGURIDAD FISICA

- ✓ Iluminación de protección.
- ✓ Sistemas de alarma y detección de intrusos.
- ✓ Sistemas de barreras.
- ✓ Entradas físicas y control de accesos.
- ✓ Sistemas de video vigilancia.
- ✓ Sistemas de comunicación.
- ✓ Personal de protección.



ILUMINACIÓN DE PROTECCIÓN

1. OBJETIVOS PRIMARIOS:

- ✓ Debe actuar como disuasivo de intrusos.
- ✓ Si se presenta una intrusión, debe facilitar la detección.
- ✓ No debe exponer innecesariamente al personal de patrullaje.

2. CONSIDERACIONES EN DISEÑO:

- ✓ Todo acceso exterior a la lámpara debe estar bajo una cubierta resistente.
- ✓ Antes de tomar cualquier decisión sobre la instalación de la iluminación considere el impacto que la iluminación tendrá en su vecindario.
- ✓ Antes de utilizar cualquier estándar sugerido, verifique con las leyes locales.

3. TIPOS DE SISTEMAS DE ILUMINACIÓN.

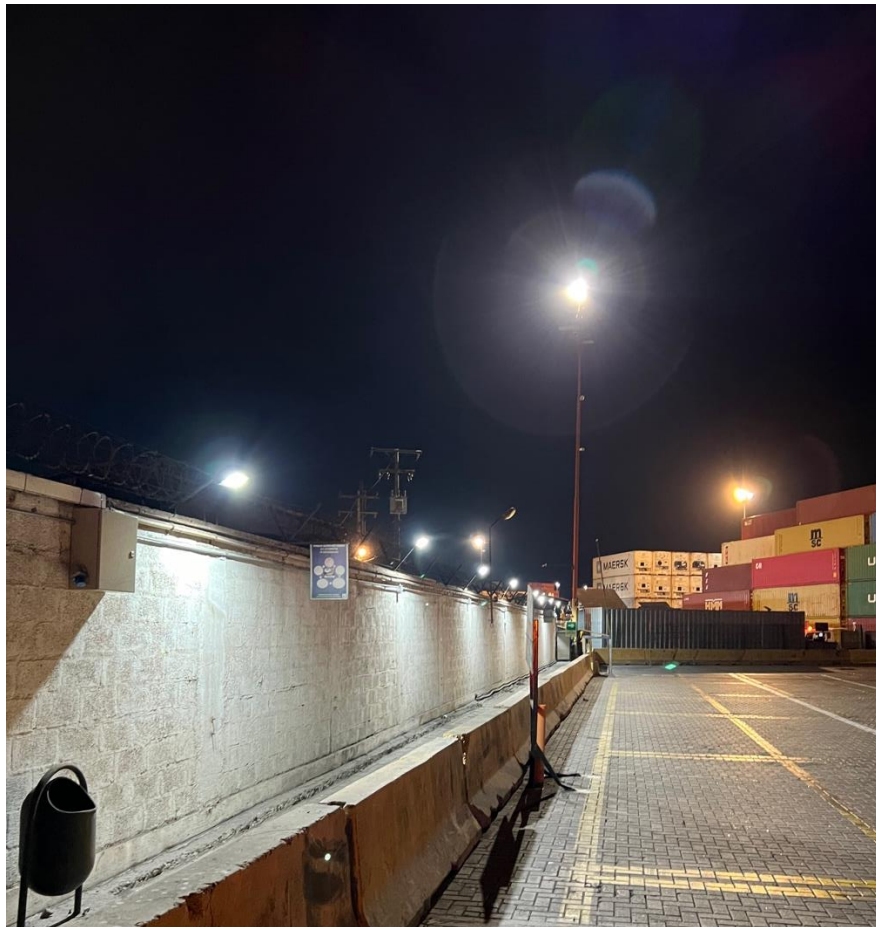
- ✓ **Luz continua** – Es el tipo de luz usada más comúnmente, las lámparas son aseguradas en su sitio y son normalmente iluminados en horas de la noche.
- ✓ **Luz de emergencia** – Es diferente a la luz continua, ya que las lámparas se encienden solo cuando son requeridas.
- ✓ **Luz móvil**– Es portátil, puede ser usada para suplir la luz continua o cuando falla la de emergencia

ILUMINACIÓN DE PROTECCIÓN

- ❖ La luz incandescente.
- ❖ Las lámparas de descarga gaseosa
- ❖ Las lámparas de cuarzo
- ❖ Las lámparas LED



ILUMINACIÓN DE PROTECCIÓN



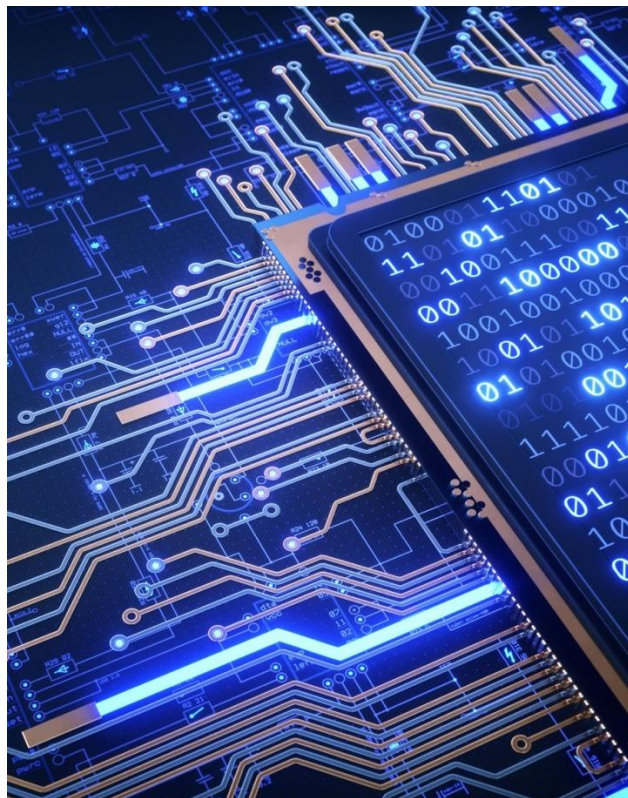
ILUMINACIÓN DE PROTECCIÓN

Indudablemente la cantidad de iluminación recomendada para situaciones específicas varía, y se mide en foot candle (Fc.) o en lux, siendo la iluminación recomendada:

Límite del perímetro o propiedad	0.15 a 0.4 Fc. ~ 1.6 lux a 4.2 lux
Entradas de vehículos	1.0 Fc. ~ 10.8 lux
Entradas peatonales	2.0 Fc. ~ 21.5 lux
Exterior de edificios	1.0 Fc. ~ 10.8 lux
Patios abiertos	0.2 Fc. ~ 2.1 lux



SISTEMAS DE ALARMAS Y DETECCION DE INTRUSOS



La seguridad física utiliza las personas, los procedimientos y la tecnología (hardware y software) para proteger activos.

Los componentes de hardware de un PPS incluyen sensores, cámaras, iluminación, monitoreo de alarmas dispositivos de equipos, control de entrada y salida, barreras y equipos de vigilancia, tales como radios, esposas, dispositivos de coacción y armas.

Las personas, los procedimientos y la tecnología se combinan para proveer las funciones de un PPS.

Las principales funciones de un PPS son la detección, la demora y la respuesta, una función secundaria es la disuasión (García, 2008, pp 2-6).

SISTEMAS DE ALARMAS Y DETECCION DE INTRUSOS

DETECCION:

- ✓ Entrada no autorizada.
- ✓ Movimientos internos no autorizados.
- ✓ Accesos no autorizados para controlar áreas u objetos.

COMPONENTES PARA EL SISTEMA DE DETECCIÓN DE INTRUSOS

- ✓ Detectores / sensores.
- ✓ Sistemas de Control.
- ✓ Transmisión de señal.
- ✓ Sistema de Monitoreo.



SISTEMAS DE ALARMAS Y DETECCION DE INTRUSOS

DETECTOR / SENSORES

- ✓ **Interruptores magnéticos.**
- ✓ **Aluminio metálico.**
- ✓ **Vibración.**
- ✓ **Ultrasonido.**
- ✓ **Fotoeléctrico.**
- ✓ **Infrarrojo pasivo.**
- ✓ **Microondas.**



SISTEMAS DE ALARMAS Y DETECCION DE INTRUSOS

SISTEMAS DE CONTROL

El **equipo de procesamiento de datos** básicamente actúa como un receptor que interpreta las señales emitidas por los sensores/detectores y reacciona de acuerdo a instrucciones previamente programadas.

- a) Restringir el acceso a las personas no autorizadas en ciertas horas y/o días de la semana.
- b) Controlar el acceso dentro de las áreas seleccionadas después de horas de oficina.
- c) Control de acceso a un parqueadero después de las horas de oficina.
- d) Controlar selectivamente el uso de elevadores.
- e) Mantener un registro de todo el uso válido e inválido de tarjetas.
- f) En caso de requerirse, en cualquier momento se podrá presentar un listado del personal presente en la propiedad.

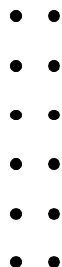
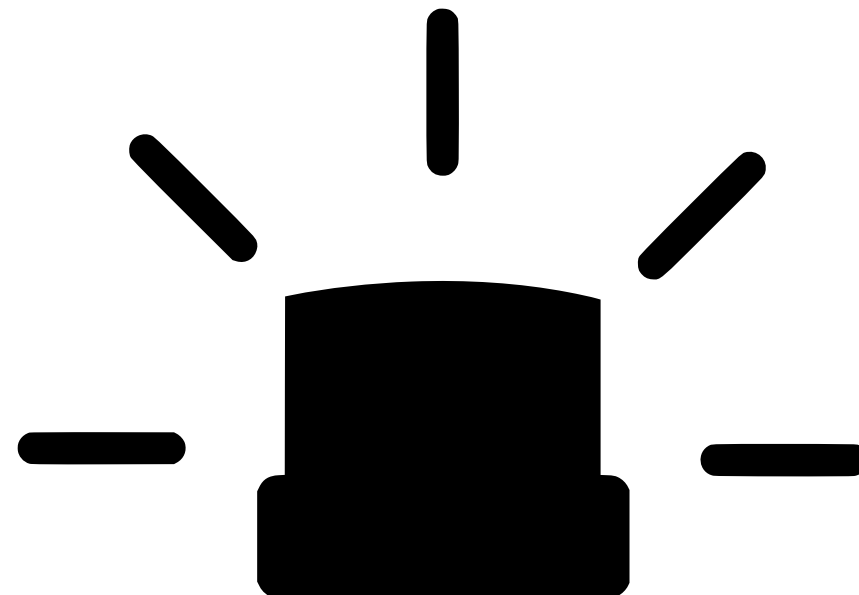


SISTEMAS DE ALARMAS Y DETECCION DE INTRUSOS

TRANSMISIÓN DE LA SEÑAL

Se denomina **transmisión de señal** a la manera por la cual un sistema de detección de intrusos comunica los sensores, sistema de control y monitoreo; puede ser de manera inalámbrica y alámbrica.

El equipo puede simplemente activar una sirena local o puede enviar una señal al teléfono del propietario o de la unidad responsable del monitoreo y reacción al otro lado del mundo.



SISTEMAS DE ALARMAS Y DETECCION DE INTRUSOS

SISTEMA DE MONITOREO

El **sistema local** es solo una sirena o un “anunciador” en el exterior de las zonas protegidas.

El **sistema propietario** es similar a un sistema local, con la diferencia de que el sistema está supervisado mediante una central de alarma en el sitio o remotamente.

El **monitoreo externo** cae en dos categorías: estaciones de monitoreo comercial o servicio de respuesta público. El monitoreo externo utiliza generalmente señales transmitidas por línea telefónica o vía IP (Web).

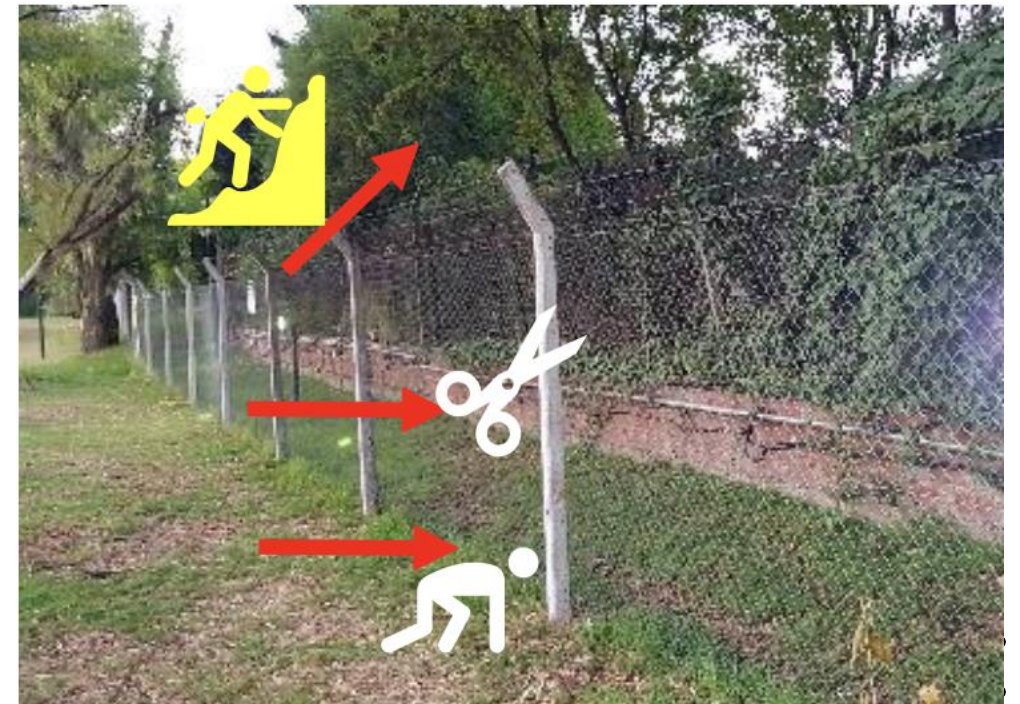


SISTEMAS DE BARRERAS

MALLA ESLABONADA

- ✓ 7 pies ~ 2,20 mts. en altura sin considerar la proyección superior.
- ✓ El alambre debe tener calibre # 9 ~ diámetro de 3,7 mm. o mayor.
- ✓ Las aberturas del acoplamiento no deben ser mayores de 4 pulgadas² ~ 25 cms².
- ✓ La malla se debe sujetarse al metal rígido o a los postes de concreto reforzados.
- ✓ No debe haber más de dos pulgadas ~ 5 cms. entre la base de la cerca y el piso.
- ✓ Donde la tierra esté suave o arenosa, la malla de la cerca debe extenderse bajo la superficie.
- ✓ La proyección superior debe hacer frente hacia fuera y hacia arriba a un ángulo de 45 grados.
- ✓ Los brazos de soporte de la proyección deben soldarse a la base superior de los postes de la cerca.
- ✓ La proyección debe aumentar la altura total de la cerca por un pie ~ 30.5 cms.
- ✓ En los brazos soporte se colocarán 3 líneas de alambre de púas, espaciados en 6 pulgadas ~ 15,2 cms.
- ✓ Una zona libre de 20 pies ~ 6 metros o más debe existir entre el perímetro y jardineras o estructuras exteriores.
- ✓ En lo posible, una zona libre de 50 pies ~ 15.20 mts o más debe existir entre el perímetro y estructuras o edificios dentro del área protegida.

SISTEMAS DE BARRERAS



SISTEMAS DE BARRERAS

PAREDES, MUROS, PISOS Y TECHOS

Las paredes pueden estar hechas de materiales como:

- ❖ Ladrillo, piedra, bloque de hormigón o ladrillo de vidrio.
- ❖ Particularmente los de hormigón, pueden ser reforzados con barras de acero (verticales, horizontales o grilla).
- ❖ Deben ser lo suficientemente altos como para disuadir a las personas de trepar sobre ellas y deben cubrirse con materiales que dificulten que se escale (cerco eléctrico, concertina, alambres de púas o puntas metálicas)
- ❖ Los pisos y techos también son importantes si pueden ser usados como rutas de ataque desde el exterior (espacios adyacentes o acometidas de servicios) hacia los activos a proteger, por lo que también deben ser reforzados con barras de acero al igual que las paredes.
- ❖ Los pisos tienden a ser más robustos que los techos ya que deben soportar todo el peso de la estructura.

SISTEMAS DE BARRERAS

PAREDES, MUROS, PISOS Y TECHOS



SISTEMAS DE BARRERAS

CERCOS ELECTRICOS

Consisten en líneas de alambre soportadas por postes equipados con aisladores.

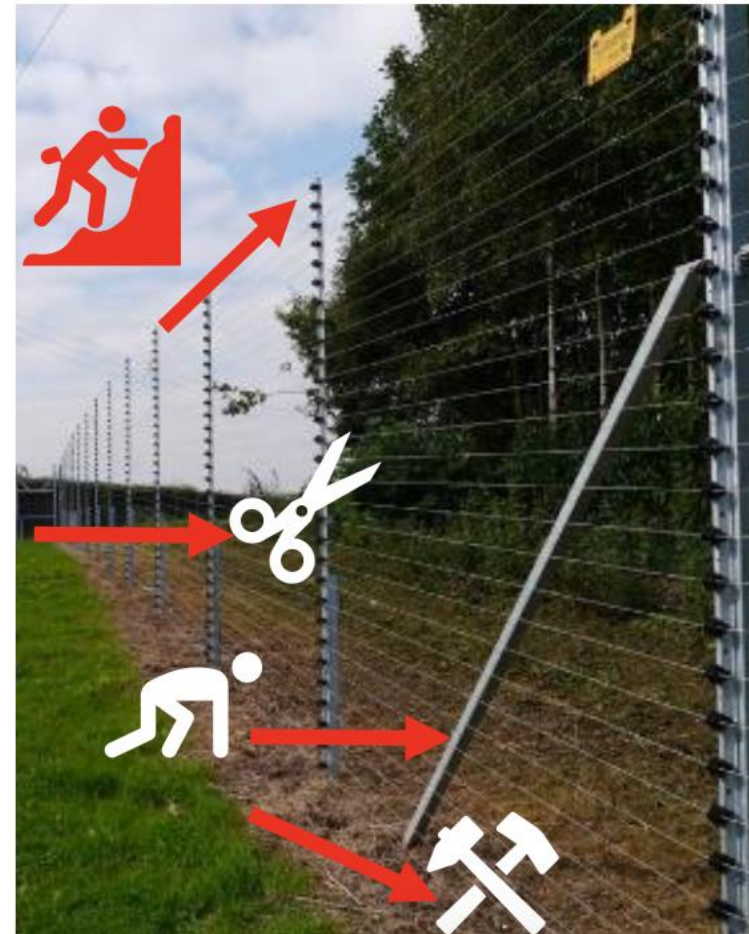
- ✓ Pueden ser sistemas simples de 5 cables como tope anti escalamiento de una pared, o de varias zonas con hasta 50 cables para sitios de alta seguridad.
- ✓ La mayoría de las aplicaciones industriales tienen una altura de 2,4 m con 20 cables y están instaladas en el interior de una cerca perimetral común o un sistema de doble cerca.
- ✓ No son letales pero si desagradables para el delincuente que elige hacer contacto. No usan corriente eléctrica; en cambio, la energía eléctrica en forma de "pulso" se descarga en el alambre aproximadamente 45 veces por minuto.

❖ Vienen en dos formas:

- ✓ Común: alambres con pulso, funciona basado en el miedo humano a una descarga eléctrica
- ✓ Monitoreado: adicionalmente el cerco detecta el corte o escalada de los alambres y activará una alarma.
- ✓ Generalmente se integran con sistemas de detección de intrusos y cada video vigilancia.

SISTEMAS DE BARRERAS

CERCOS ELECTRICOS



SISTEMAS DE BARRERAS

CRISTALES

Los siguientes son algunos tipos diferentes de vidrio de ventana:

El vidrio recocido (común) se ha fabricado mediante un proceso de enfriamiento lento	El vidrio recocido se rompe en fragmentos grandes que pueden causar lesiones graves, y los códigos de construcción pueden restringir su uso en lugares donde existe un alto riesgo de rotura y lesiones, como paneles de puertas y salidas de incendios.
El vidrio templado se trata para resistir la rotura.	Los códigos de construcción requieren vidrio templado por razones de seguridad porque cuando el vidrio se rompe, se fragmenta en pedazos pequeños en lugar de fragmentos.
El vidrio con alambre proporciona resistencia contra objetos grandes, pero aún puede romperse.	A menudo se requiere por códigos de incendio para ciertas ventanas (utilizado para mantener la clasificación de resistencia al fuego en puertas con clasificación de resistencia al fuego).
El vidrio laminado se compone de dos láminas de vidrio ordinario unidas a una capa intermedia o capas de material de láminas de plástico.	Cuando el vidrio laminado está estresado o golpeado, puede romperse y romperse, pero las piezas de vidrio tienden a adherirse al material plástico. Debe notarse que para que el vidrio laminado sea efectivo, debe instalarse en un marco y el marco asegurado a la estructura. También es el tipo de vidrio preferido para mitigar las fuerzas de explosión. Ayudará en la protección de los ocupantes del edificio contra la rotura de cristales en caso de explosión.
El vidrio antibalas o antirrobo proporciona una mayor resistencia al ataque.	Está laminado y consta de múltiples capas de vidrio, policarbonato y otras películas de plástico para proporcionar muchos niveles de resistencia balística.

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

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



INTERNATIONAL
FOUNDATION FOR
PROTECTION OFFICERS
KNOWLEDGE TO PROTECT

SISTEMAS DE BARRERAS

Barrotes:

- Pueden proteger la abertura de la ventana para que no se use como punto de acceso.

Film protector (retención de fragmentos)

- Se adhiere a la superficie interior del vidrio, fortalece y mantiene el vidrio en su lugar si se rompe, y puede lograr varios otros propósitos:
- Proporciona diversos grados de protección contra intrusiones tipo “ruptura y robo”.
- Se puede derrotar con ataques repetidos (dependiendo del grado de protección).
- Reduce las lesiones causadas por fragmentos de vidrio de proyectil en caso de explosión o clima extremo (es decir, huracán o tornado)

Cortinas anti – explosivas

- Están hechas de telas reforzadas que brindan protección contra materiales voladores en una explosión.
- Las cortinas anti - explosivas no protegen una instalación contra intrusiones, pero protegen a las personas y activos de daños.

Persianas de seguridad

- Mejoran la protección de ventanas.
- Tipo enrollable, con listones de enclavamiento horizontales (generalmente de aluminio o cloruro de polivinilo) que enrollan una caja ubicada en la parte superior de la ventana.
- Tipo acordeón, con laminas verticales entrelazadas que se deslizan hacia los lados de la ventana.
- Estas persianas se pueden operar manualmente o eléctricamente usando controles remotos, sensores meteorológicos o temporizadores.

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

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

SISTEMAS DE BARRERAS

CAJAS FUERTES Y BOVEDAS

Las cajas fuertes y bóvedas son diseñadas para ofrecer variados niveles de protección a partir de riesgos específicos, allanamientos, robos e incendios

Los dos tipos de cajas fuertes de mayor interés son la caja fuerte de registros (a prueba de incendio) y la caja fuerte de dinero (resistente al robo).

Cerraduras - Las cajas fuertes están disponibles con tres tipos de sistemas de trabas.

Clave – una persona con la clave puede acceder a los contenidos en cualquier momento.

Clave con llave – es más compleja ya que requiere de dos personas para abrir el seguro, la una manipula la llave para quitar el seguro y la otra pone la clave para quitar la protección.

- • Seguro combinado dual – es similar a la segunda opción en la que dos personas deben acordar para abrir el seguro, cada persona tiene una combinación única.

- •
- •
- •
- •
- •
- •

- •
- •
- •
- •
- •
- •

SISTEMAS DE BARRERAS

CAJAS FUERTES Y BOVEDAS

Las cajas fuertes y bóvedas son diseñadas para ofrecer variados niveles de protección a partir de riesgos específicos, allanamientos, robos e incendios

Los dos tipos de cajas fuertes de mayor interés son la caja fuerte de registros (a prueba de incendio) y la caja fuerte de dinero (resistente al robo).

Cerraduras - Las cajas fuertes están disponibles con tres tipos de sistemas de trabas.

Clave – una persona con la clave puede acceder a los contenidos en cualquier momento.

Clave con llave – es más compleja ya que requiere de dos personas para abrir el seguro, la una manipula la llave para quitar el seguro y la otra pone la clave para quitar la protección.

- • Seguro combinado dual – es similar a la segunda opción en la que dos personas deben acordar para abrir el seguro, cada persona tiene una combinación única.

SISTEMAS DE BARRERAS

CAJAS FUERTES Y BOVEDAS

- ORGANIZACIONES INTERNACIONALES DE
- CERTIFICACION DE CALIDAD
- U.L. UNDERWRITES LABORATORIES INC.
- ISO INSURANCE SERVICE OFFICE
- ASTM AMERICAN SOCIETY FOR TESTING AND MATERIALS
- ANSI AMERICAN NATIONAL STANDARDS INSTITUTE
- BPA BANK PROTECTION ACT

- CLASIFICACIÓN POR TIPO DE ATAQUE
- TL = TOOL RESISTANT SAFE
- TR = TORCH RESISTANT
- TX = TORCH EXPLOSIVE
- TL = TIEMPO DE APETURA CON HERRAMIENTAS MECANICAS
O ELECTRICAS DE 6"2
- TR = TIEMPO DE APERTURA CON OXIACETILENO 2"2



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

SISTEMAS DE BARRERAS

OTRAS CONSIDERACIONES CAJAS FUERTES Y BOVEDAS

- ✓ Cerraduras
- ✓ Depositarios
- ✓ Cerraduras temporales
- ✓ Cerraduras de tiempo
- ✓ Dispositivos de reaseguramiento
- ✓ Peso extra
- ✓ Anclamiento al piso
- ✓ Bóvedas resistentes a robos
- ✓ Contenedores resistentes a fuego.



ENTRADAS FISICAS Y CONTROL DE ACCESO

CONTROL DE ACCESO :

Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos de negocio y de seguridad

Fuente:

Norma ISO 27000, Sistemas de Gestión de la Seguridad de la Información

1. Accesos perimetrales.
2. Accesos que controlan y restringen movimientos internos.
3. Accesos hacia áreas sensitivas y restringidas.



ENTRADAS FISICAS Y CONTROL DE ACCESO

CERRADURAS:

Las cerraduras pueden ser mecánicas, eléctricas, y electromecánico.

Las cerraduras de embutir con pestillo deben ser consideradas de seguridad, el pestillo debe medir por lo menos 1 pulgada, es decir 2,5 cms.

Las cerraduras electricas y electromecánicas, tienen dos posiciones: Bloqueada o abierta y son configuradas para permanecer trabados en falla o destrabados en falla.

- Control remorto para la puerta de entrada de peatones.
- Puertas de salida de emergencia.
- Puertas de emergencia desde escaleras a la base.
- Todas las puertas de escaleras.
- Además, se pueden abrir con llaves.



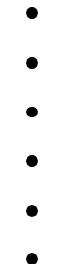
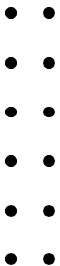
ENTRADAS FISICAS Y CONTROL DE ACCESO

CERRADURAS EN SALIDAS DE EMERGENCIA:

Reguladas en nuestro país por el DS N° 47 de Ministerio de Vivienda y Urbanismo, establece Reglamento de seguridad contra incendios en los edificios.

Mínimo al menos 71 cms (28 pulgadas de ancho) .

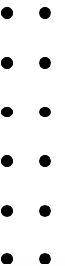
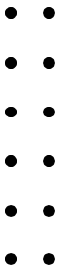
Las puertas de emergencia no pueden abrirse en contra del sentido de la evacuación y los accesos señalizados y libres de obstrucciones, pueden estar semicerradas, pero nunca con llaves u otro que impida su fácil apertura.”



ENTRADAS FISICAS Y CONTROL DE ACCESO

AL USAR CERRADURAS ELECTRICAS O ELECTROMAGNETICAS EN SALIDAS DE EMERGENCIA:

- ✓ La cerradura debe poder abrir de manera manual desde el interior, para egresar sin esfuerzo.
- ✓ Debe existir un centro de control las 24 H en la propiedad protegida.
- ✓ El centro de control debe poder activar y desactivas.
- ✓ La activación del sistema de alarma de fuego debe desactivar el dispositivo de seguridad.
- ✓ Los accesos a estaciones para control de fuego deben tener cerraduras que desactiven automáticamente.



ENTRADAS FISICAS Y CONTROL DE ACCESO

PARA PROTEGER SALIDAS DE EMERGENCIA:

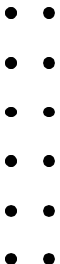
- ✓ Barras horizontales de protección para puertas dobles que abran sin llave solo del interior.
- ✓ Cerradura de pestillo con tiempo de retardo de apertura.
- ✓ Los dispositivos de salidas de emergencia pueden estar conectadas a una CRA.



ENTRADAS FISICAS Y CONTROL DE ACCESO

CONTROL DE LLAVES:

Es un procedimiento altamente crítico



SISTEMAS DE VIDEO – VIDEO VIGILANCIA

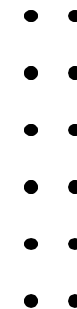
❖ Componentes básicos de un sistema CCTV:

- ✓ Cámara
- ✓ Cubierta
- ✓ Monitor
- ✓ Interruptor secuencial
- ✓ Detectores de movimiento
- ✓ Control de paneo/inclinación/acercamiento (PTZ)
- ✓ Controles
- ✓ Grabador de video
- ✓ Generador de día/hora
- ✓ Consola.



REFERENCIAS A CONSULTAR

- ✓ American Military University. (n.d.). Security management. Consultado de https://start.amu.apus.edu/securitymanagement/overview?gclid=Cj0KCQjw3JXtBRC8ARIsAEBHg4mzTWn3wYcC5FjmHObbdc9kdnFQAM1sxijXeou_Dr9GYwHnho7uUDAAaAkGbEALw_wcB#school=sgs.
- ✓ ASIS International. (n.d.-a). Scholarship and grant opportunities. Consultado October 14, 2019, de <https://www.asisonline.org/get-involved/asis-foundation/foundationships-and-grants/>.
- ✓ ASIS International. (n.d.-b). ASIS Board Certifications. Consultado May 29, 2019, de <https://www.asisonline.org/certification/asis-board-certifications2/>.
- ✓ FindAMasters. (n.d.). Distance learning masters degrees in criminology. Consultado October 15, 2019, de <https://www.findamasters.com/masters-degrees/criminology/distance-learning/?32gosej0>.
- ✓ National Institute of Standards and Technology (NIST). (2001, May 25). FIPS 140-2, Security requirements for cryptographic modules. Consultado de <https://csrc.nist.gov/publications/detail/fips/140/2/final>.
- ✓ Purdue University Global | IFPO. (2018). Consultado May 30, 2019, de <https://go.purdueglobal.edu/els/ifpo/>.



FUNDAMENTOS DEL SISTEMA DE ALARMA

Manual CPO.



CPO®

INTRODUCCIÓN

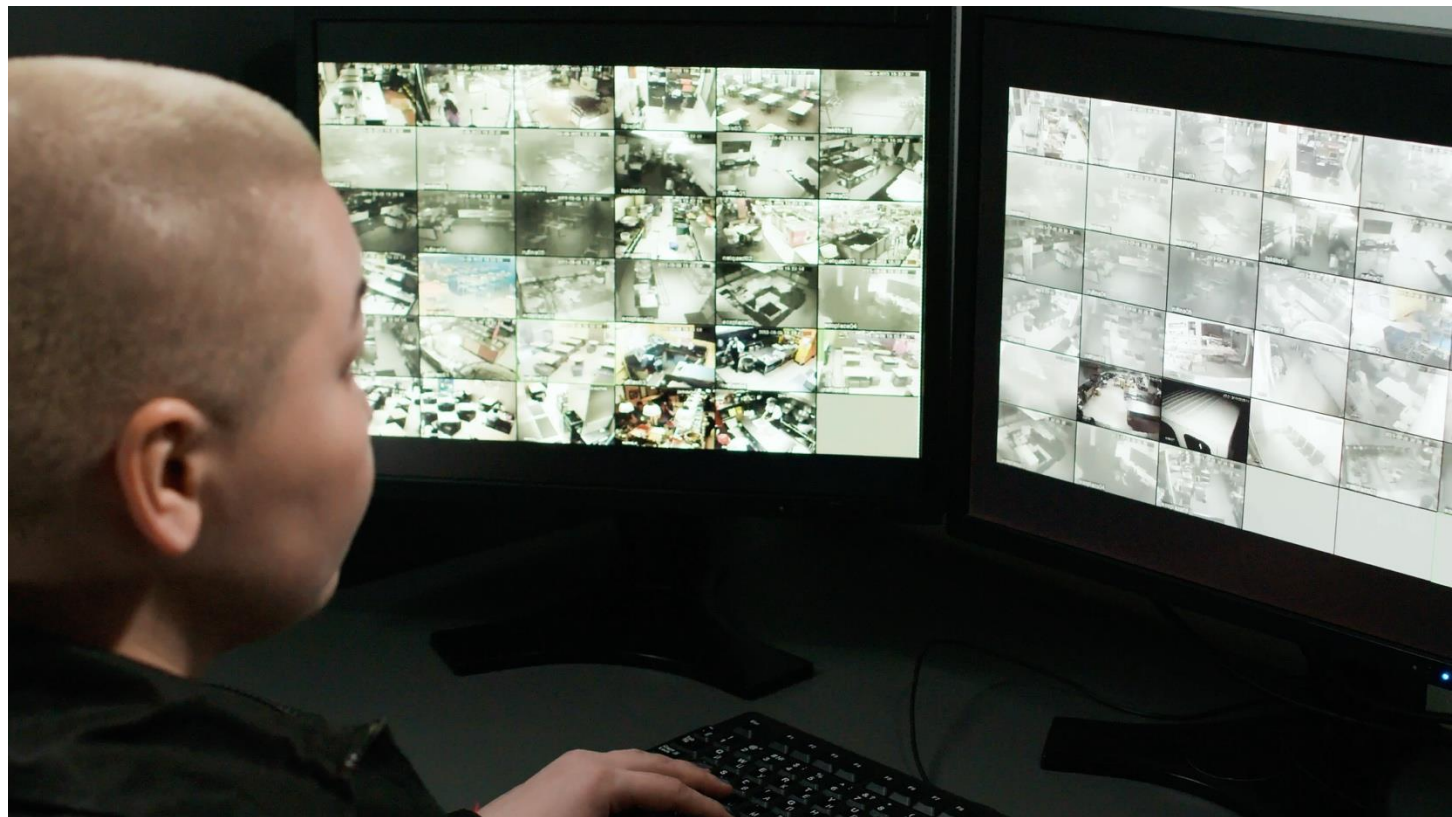


Un sistema de alarma correctamente diseñado resulta la piedra angular de un sistema de detección en un programa de protección física. Estos mecanismos tecnológicos pueden interactuar y complementar su eficacia con elementos de monitoreo como el cctv e iluminación. Como se puede observar una alarma resulta crucial para cualquier planificación que deseemos llevar adelante.

FUNDAMENTOS DEL SISTEMA DE ALARMAS

Monitoreo de alarmas:

- ✓ Monitoreo local
- ✓ Estación de monitoreo propietario
- ✓ Estación comercial de monitoreo
- ✓ Monitoreo policial.



OPERADOR DE CCTV



SENSORES DE ALARMA GENERAL

Los sensores de uso general en el perímetro se dividen en 3 capas: protección de perímetro, protección de áreas y protección del punto.

- ❖ Sensor ultrasónico o vidrios rotos.
- ❖ Interruptor magnético balanceado.
- ❖ Sensor de rejilla-alambre.



SENSORES DE ALARMA VOLUMÉTRICOS

Los sensores de protección de áreas incluyen:

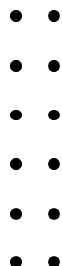
- ❖ Sensores de movimiento de microondas
- ❖ Sensor infrarojo pasivo
- ❖ Sensor de tecnología dual.
- ❖ Sensor de movimiento en video.



SENSORES DE ALARMA DE PUNTO

Los sensores de protección de áreas incluyen:

- ❖ Sensores de capacitancia
- ❖ Sensor de vibración.
- ❖ Sensor de presión.



FALSAS ALARMAS Y DETECCION ERRADA

Las falsas alarmas pueden ser:

- ❖ Uso incompetente.
- ❖ Mala instalación.
- ❖ Falta de mantenimiento
- ❖ Materiales deficientes.
- ❖ Empleados indiferentes.



RESPUESTAS DE ALARMA

Si hay detección, debe existir una verificación, la respuesta ante un incidente de seguridad debe ser generada por el propio personal de seguridad o las autoridades de emergencias.

Sugerencias:

- ✓ Nunca asuma que un evento de alarma es nada. Asuma que se responde a una intromisión hasta que se comprueba lo contrario.
- ✓ Mantener contacto radial constante con el oficial y la CRA.
- ✓ Mantenga la disciplina, mantenga radio con volumen bajo.
- ✓ Si a su llegada hay cristales rotos, no ingrese al edificio.



REFERENCIAS A CONSULTAR

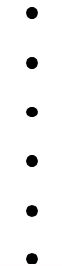
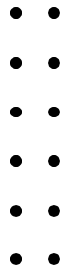
- ✓ Nelson, L. A. (1999). Designing operations centers. S. J. Davies, & R. R. Minion (Eds.), (2nd ed.). Security supervision: Theory and practice of asset protection (pp. 277–279). Burlington: Elsevier Science.
- ✓ Ruiz, H. C. (1999). Security technologies. S. J. Davies, & R. R. Minion (Eds.), (2nd ed.). Security supervision: Theory and practice of asset protection (pp. 263–271). Burlington: Elsevier Science.

CONTROL DE ACCESO Y VIDEO VIGILANCIA

El control de Acceso de una instalación, representa un reto para toda las áreas de la organización, parece algo sencillo, pero es una tarea ardua que exige de política, procedimientos, protocolos y del compromiso de toda la iorganización para que se cumpla sus objetivos.

El control de acceso no es llegar y abrir una puerta para el ingreso de un auto o persona. Esta simple acción puede poner en jaque a personas, información, los activos y la reputación de la empresa.

Por ende debe ser de extrema preocupación para cualquier organización ya que representa la medida de control más fuerte que debe existir en una compañía.



PERSONAL PARA CONTROL DE ACCESO



CONTROL DE ACCESO EN EMERGENCIAS



PROCEDIMIENTO DE CONTROL DE ACCESO



VALIDAR Identidad con algo que tiene, es o sabe.

CONFIRMAR Derecho de acceso contrastando con una lista.

REGISTRAR acceso o intento de acceso.

INSPECCIONAR Las propiedades con las que ingresa.

ENTREGAR información adicional y restricciones del lugar.

PERMITIR acceso.

SISTEMAS ELECTRÓNICOS PARA EL CONTROL DE ACCESO

Los sistemas electrónicos de control de acceso deben tener las siguientes capacidades:

- ✓ Restringir el acceso a las personas no autorizadas en ciertas horas y/o días de la semana.
- ✓ Controlar el acceso dentro de las áreas seleccionadas después de horas de oficina.
- ✓ Control de acceso a un parqueadero después de las horas de oficina.
- ✓ Controlar selectivamente el uso de elevadores.
- ✓ Mantener un registro de todo el uso válido e inválido de tarjetas.
- ✓ En caso de requerirse, en cualquier momento se podrá presentar un listado del personal presente en la propiedad.

SISTEMAS ELECTRÓNICOS PARA EL CONTROL DE ACCESO

Tipos de tarjetas para sistemas electrónicos de control de acceso:

- ✓ RFD
- ✓ Tarjeta de proximidad
- ✓ Codificada magnética
- ✓ Franja codificadora magnética.
- ✓ Codificada weingand
- ✓ Hollerith
- ✓ Óptica codificada.



La información contenida en la tarjeta de identificación del empleado puede ser fácilmente incorporada en cualquier tarjeta de acceso, imprimiendo datos básicos como: Nombre de la Compañía y logotipo, detalles del titular de la tarjeta, nombre, cargo, fecha de nacimiento, firma, fotografía, condiciones de uso (restricciones).

No se recomienda registrar departamento o derechos de acceso, ya que en caso de pérdida la tarjeta podría ser usada en la dependencia y accesos declarados.

SISTEMAS DE CAMARAS CCTV

CCTV es el acrónimo para Circuito Cerrado de Televisión (o Closed Circuit Television). La expresión “Circuito Cerrado” quiere decir que se trata de una instalación de componentes directamente conectados, que crean un circuito de imágenes que no puede ser visto por otra persona fuera de él. Y se diferencia de la emisión de señales de televisión ordinarias en que éstas pueden ser vistas por cualquiera con una antena u otro equipo para recibirlas, mientras que el CCTV no.



FUNCIONAMIENTO DE SISTEMAS DE CAMARAS CCTV



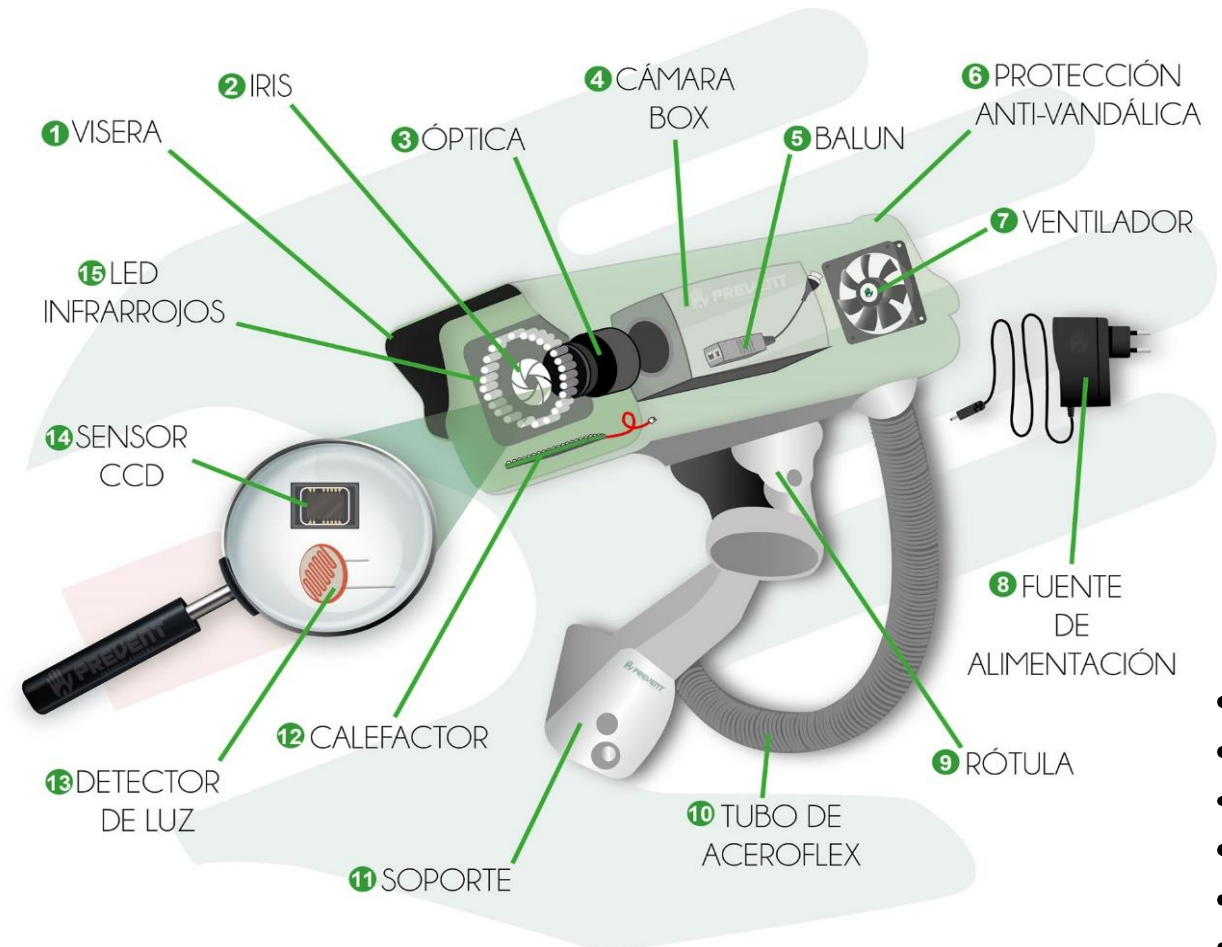
Sistemas análogos
Sistemas Digitales.
Sistemas híbridos.

“Hoy la video analítica y la implementación de la IA, están conduciendo las prestaciones de los equipos de cctv a niveles insospechados.”

DVR

Son sistemas de administración de videos y g

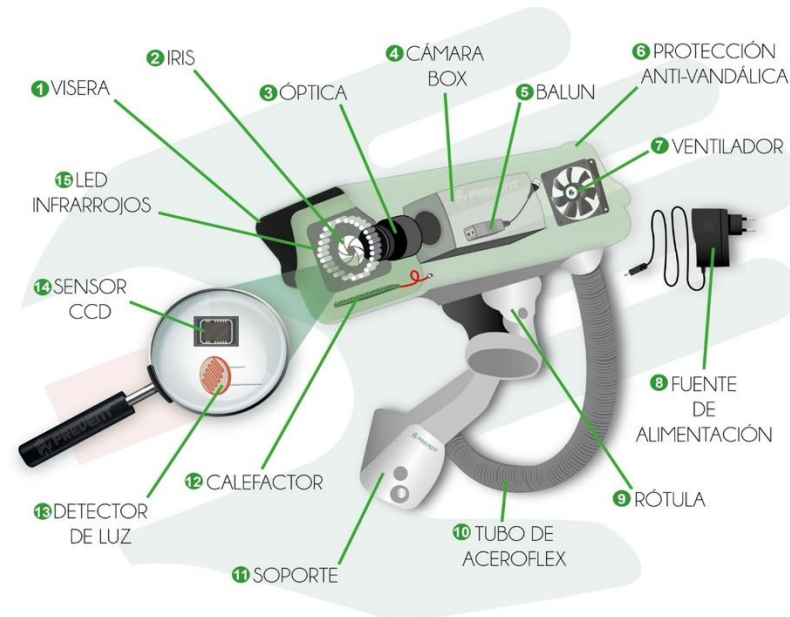
El medio físico más usado para transmisión d
es el cable coaxial; sin embargo, el uso de
video-balun's es cada vez más común por el
al coaxial.



DVR

Son sistemas de administración de videos y grabación.

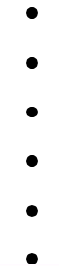
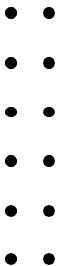
El medio físico más usado para transmisión de la señal de video análoga entre la cámara y el DVR es el cable coaxial; sin embargo, el uso de cable par trenzado (UTP), más la implementación de video-balun's es cada vez más común por el menor costo que representa este tipo de cable frente al coaxial.



DVR

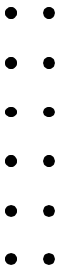
Clasificación de DVR'S

1. Número de canales o número de cámaras que se pueden conectar al equipo. Comúnmente los modelos que más se fabrican son para 4, 8, 16, 32 canales y algunas marcas fabrican modelos de 9, 24, 48 canales.
2. El tipo de tecnología que usa para los diferentes formatos de video: análogo, HDCVI, HDTVI, AHD
 - **HDCVI:** interfaz compuesta de video de alta definición desarrollada por DAHUA.
 - **HDTVI:** interfaz de transporte de video de alta definición en estándar abierto desarrollado en Silicon Valley, adoptado por HIKVISION bajo el nombre TURBO HD.
 - **AHD:** alta definición analógica desarrollado por Nextchip Korea.



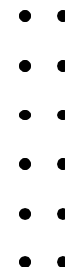
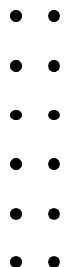
CARACTERÍSTICAS BÁSICAS AL ELEGIR UN DVR

1. Resolución.
2. Velocidad de procesamiento de imágenes.
3. Almacenamiento.
4. Formato de compresión de video.



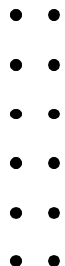
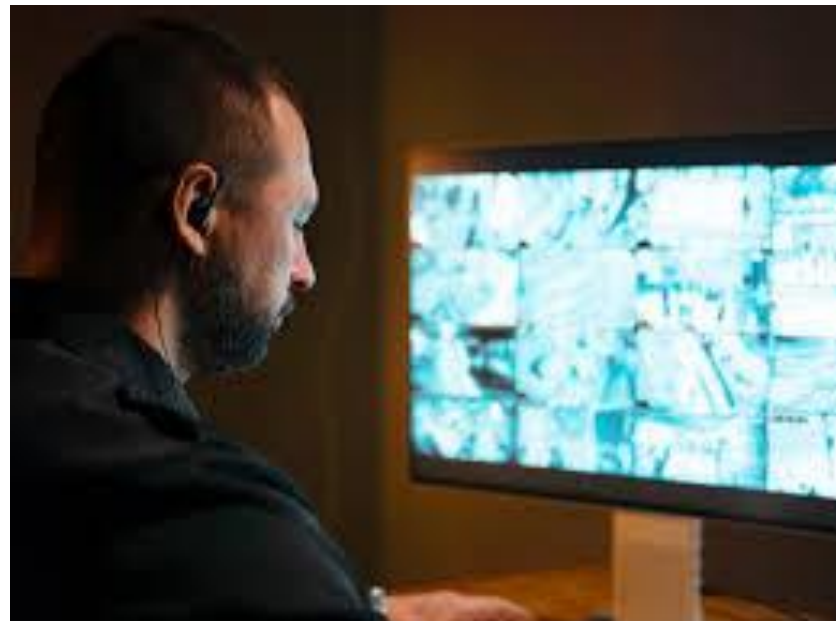
PERIFERICOS A CONSIDERAR

1. Puertos USB
2. Entradas y salidas de alarmas.
3. Puerto de RED
4. Puerto de video
5. Entradas de audio
6. Puertos RS232/RS485



MODOS DE GRABACIÓN.

1. Grabación continua.
2. Por eventos.
3. Por agenda o cronograma.



ESCENARIOS PRESENTES Y FUTUROS DE USO

