DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Fundamentos de ciberseguridad

Seguridad física y ambiental

Profesor
Juan Ignacio Iturbe A.

Introducción

- La seguridad es muy importante para cualquier compañía y su infraestructura.
- La seguridad física no es la excepción.
- El hacking no es la única forma con que la información y sus sistemas relacionados sean comprometidos.
- La seguridad física engloba su propio conjunto de amenazas y vulnerabilidades.

Introducción

- Los mecanismos de la seguridad física incluyen:
  - Diseño y disposición del lugar
  - Componentes ambientales
  - Preparación para la respuesta ante emergencias
  - Entrenamiento
  - Control de acceso
  - Detección de intrusiones
  - Protección eléctrica y ante incendios.

Introducción

- Los mecanismos de la seguridad física protegen:
  - Personas
  - Datos
  - Equipamiento
  - Sistemas
  - Instalaciones
  - Y una larga lista de activos de la compañía.

Situación actual

- Los computadores se encuentran en cualquier escritorio.
- El acceso a dispositivos y recursos esta esparcido por todo el ambiente.
- Las compañías tienen muchos armarios de cableado y salas de servidores.
- Los usuarios remotos y móviles utilizan sus computadores y recursos fuera de la instalaciones de la compañía.

Situación actual

- Robo, fraude, sabotaje, vandalismo y accidentes provocan costos elevados para las compañías.
- Ya que sus ambientes se están volviendo cada vez mas complejos y dinámicos.
- A medida que la tecnología y el ambiente se vuelven mas complejos, mas vulnerabilidades son introducidas.

VIDEO VIGILANCA

ALARMAS DETECCION DE INCENDIOS E INTRUSOS

CONTROLES DE ACCESO

CONTROLES DE RONDA

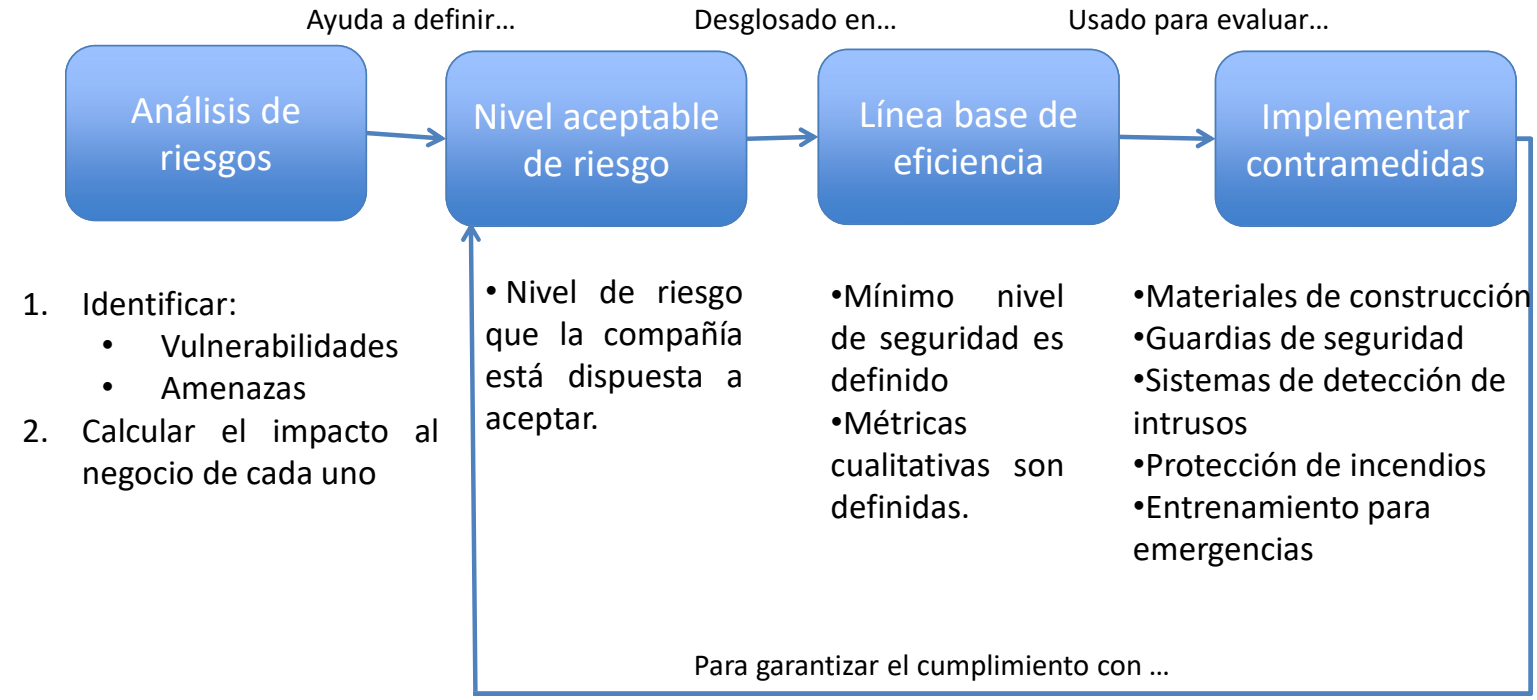
Importancia de la Seguridad Física

- Mucha gente en el campo de la seguridad de la información, no piensa acerca de la importancia de la seguridad física.
- Se enfocan en la seguridad de los computadores y su información, los hackers, puertos, virus y las contramedidas tecnológicas orientadas a la seguridad.
- La seguridad de la información sin una apropiada seguridad física es una perdida de tiempo.

Objetivos de un programa de seguridad física

- Prevención del Crimen y la alteración a través de la disuasión (ej: muros, guardias de seguridad, signos de advertencia, etc).
- Reducción del daño a través de mecanismos de retraso (ej: seguros de puertas, personal de seguridad y barreras)
- Detección del crimen y alteración (ej: Detección de humo, detectores de movimiento, CCTV)
- Evaluación de incidencia (ej: respuesta del guardia de seguridad al detectar incidentes y determinación del nivel de daño)
- Procedimientos de respuesta (ej: mecanimos de supresión de incendios, proceso de respuesta a emergencias, notificación a fuerzas policiales, consultas a profesionales de seguridad)

Proceso de planeamiento



Pasos para diseñar un programa de seguridad física

1. Identificar un equipo de empleados internos y/o consultores externos.
2. Llevar a cabo el análisis de riesgos
3. Identificar los requerimientos legales y regulatorios.
4. Trabajar con la gerencia para definir un nivel de riesgo aceptable.
5. Derivar la línea base de eficiencia desde el nivel aceptable de riesgo.

Pasos para diseñar un programa de seguridad física

6. Crear métricas de eficiencia para las contramedidas.
7. Desarrollar un criterio desde los resultados del análisis, que delinee el nivel de protección y eficiencia requerido por las siguientes categorías del programa: disuasión, mecanismos de retraso, detección, evaluación, respuesta.
8. Identificar e implementar contramedidas para cada categoría del programa.
9. Continuamente evaluar contramedidas en contra la línea base para asegurar que el nivel de riesgo aceptado no es excedido.

Amenazas sobre la seguridad física

- Amenazas a la seguridad física vienen en diferentes formas como:
  - Desastres naturales
  - Situaciones de emergencia
  - Amenazas causadas por el hombre
- Todas las posibles amenazas deben ser identificadas para realizar un completo y exhaustivo análisis de riesgos.

Amenazas sobre la seguridad física

- Algunas de las amenazas mas comunes son:
  - Incendio
  - Agua
  - Vibración y movimiento
  - Clima severo
  - Electricidad
  - Sabotage/terrorismo/guerra/robo/vandalismo
  - Falla de equipamiento
  - Perdida de comunicaciones
  - Perdida de personal

Incendios

- Amenazas como incendios pueden ser devastadoras y letales.
- Precauciones, preparación y entrenamiento apropiado, no solamente a ayuda a limitar las perdidas, sino que mas importante, a salvar vidas.
- Salvar vidas humanas es la primera prioridad en cualquier situación

Incendios

- Otros desastres asociados con incendios son: humo, explosiones, colapso de edificios, liberación de materiales tóxicos o vapores y daño por el agua.
- Para que un incendio se produzca, necesita tres elementos (triangulo del fuego): calor, oxigeno y combustible.
- Los sistemas de supresión y extinción de incendios atacan removiendo uno de estos tres elementos o rompiendo temporalmente la reacción química de estos tres elementos.

Clasificación de incendios

Clase	Descripción (combustible)	Metodo de extinción
A	Combustibles comunes, como papel, madera, muebles y ropa.	Agua y acido sodio
B	Combustibles líquidos, como gasolina o aceite.	CO2, acido sodio, o gas extintor
C	Incendios por electricidad, por computadores o electrónica	CO2 o gas extintor (Nota: El paso mas importante para combatir el fuego en esta clase es primero ¡apagar la electricidad!)
D	Incendio especial, como químicos	Puede requerir inmersión total u otras técnicas especiales

Daño por Agua

- Puede ocurrir por diferentes fuentes:
  - Rotura de cañerías
  - Por los mismos bomberos al combatir un incendio.
  - Techos con goteras
  - Bebidas derramadas
  - Inundación
  - Tsunamis
- Todo esto con computadores y equipos eléctricos puede llegar a ser letal.

Vibración y movimiento

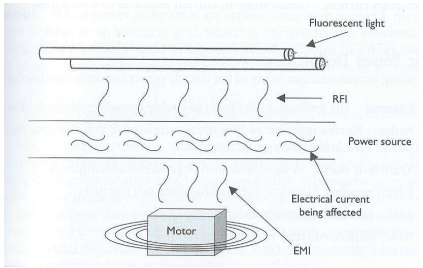
- Puede ocurrir por:
  - Terremotos
  - Deslizamiento de tierra
  - Explosiones
- Equipamiento puede ser dañado por
  - Pequeñas o grandes vibraciones.
  - Caída de objetos
  - Volcamiento de racks

Electricidad

- Equipamiento sensible puede ser dañado o afectado por vario tipos de peligros y anomalías como:
  - Descarga electroestática (ESD), la humedad en rangos:
    - Altos, causa condensación y corrosión.
    - Bajos, incrementa el potencial para ESD.
    - 40% y 60%, ideal para equipos computacionales
  - Campos magnéticos, monitores y medios de almacenamiento pueden ser permanentemente dañados o borrados por ellos.

Electricidad

- Ruido eléctrico, Incluye
  - Interferencia electromagnética (EMI), producido por las diferentes cargas de los cables positivo, neutro y tierra
  - Interferencia por radiofrecuencia (RFI), causado por componentes eléctricos, como tubos fluorescentes y cables eléctricos.
- Caída de rayos, aproximadamente en EE.UU, 10.000 incendios empiezan por caída de rayos.
- Anomalías eléctricas, siguiente tabla.



Anomalías eléctricas

Evento eléctrico	Definición
Blackout	Perdida total de energía
Falla	Momentaria perdida de energía
Apagón (Brownout)	Caída prolongada de voltaje
Caída (Sag/dip)	Caída corta de voltaje
Inrush	Alto voltaje inicial requerido para comenzar la carga de transformadores
Punta (Spike)	Momento con alto voltaje
Oleada (Surge)	Prolongado alto voltaje

Eligiendo una locación segura

- Factores importantes deben ser considerados al elegir una locación:
  - Clima y desastres naturales (ej: ¿Qué probabilidad de terremoto existe en el lugar?)
  - Consideraciones locales. (ej: ¿la locación se encuentra en una zona de alto crimen?)
  - Visibilidad (ej: ¿ tús empleados e instalaciones pueden ser objetivos para el crimen, terrorismo o vandalismo?)
  - Accesibilidad (ej: ¿Patrones de tráfico?)
  - Servicios (ej: ¿Es la electricidad estable y limpia?¿Es suficiente el cable de fibra óptica que llega al lugar para soportar los requerimientos de telecomunicación?)
  - Copropietarios (ej: ¿Pueden (y deben) compartir los copropietarios los costos y responsabilidadedes de la seguridad física?)

Diseñando una instalación segura

- Se deben considerar:
  - Muros externos
  - Muros internos
  - Pisos
  - Techos
  - Puertas
  - Iluminación
  - Cableado

Consideraciones de diseño de un sitio e instalaciones.

- Las organizaciones astutas involucran a profesionales de la seguridad durante el diseño, planeamiento, y construcción de nuevos o renovadas locaciones e instalaciones.
- Los principios de Prevención del crimen basado en el diseño del entorno (CPTED) son ampliamente adoptados en el diseño de edificios públicos y privados, oficinas… desde su primera publicación en 1971.

Consideraciones de diseño de un sitio e instalaciones.

- EL CPTED comprende tres estrategias básicas:
  - Control de acceso natural: usa zonas de seguridad para limitar o restringir el movimiento y diferenciar entre áreas publicas, semi-privadas y privadas.
  - Vigilancia natural: reduce la amenaza criminal haciendo que la actividad del intruso sea mas observable y fácilmente detectable.
  - Reforzamiento territorial: crea un sentido de orgullo y pertenencia, que causa que el intruso se destaque con mayor facilidad y alienta a las personas a denunciar actividades sospechosas

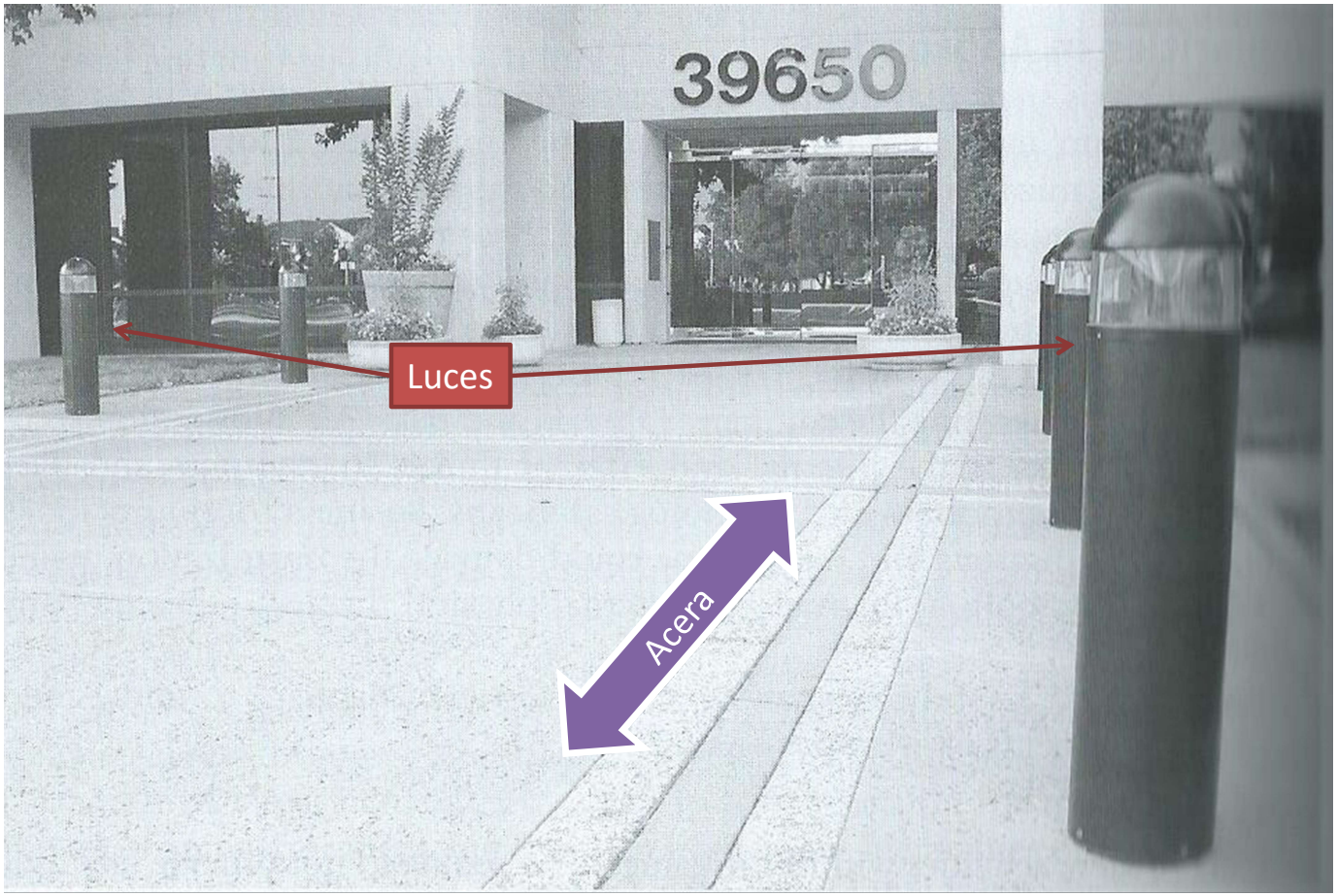
Control de acceso natural

- Se guía a la gente en la entrada y salida de un espacio por la posición de puertas, muros, luces e incluso áreas verdes.
- Las zonas pueden ser clasificadas como controladas, restringidas, publicas o sensible.
- Dependiendo de su clasificación, es el tipo de control necesario.

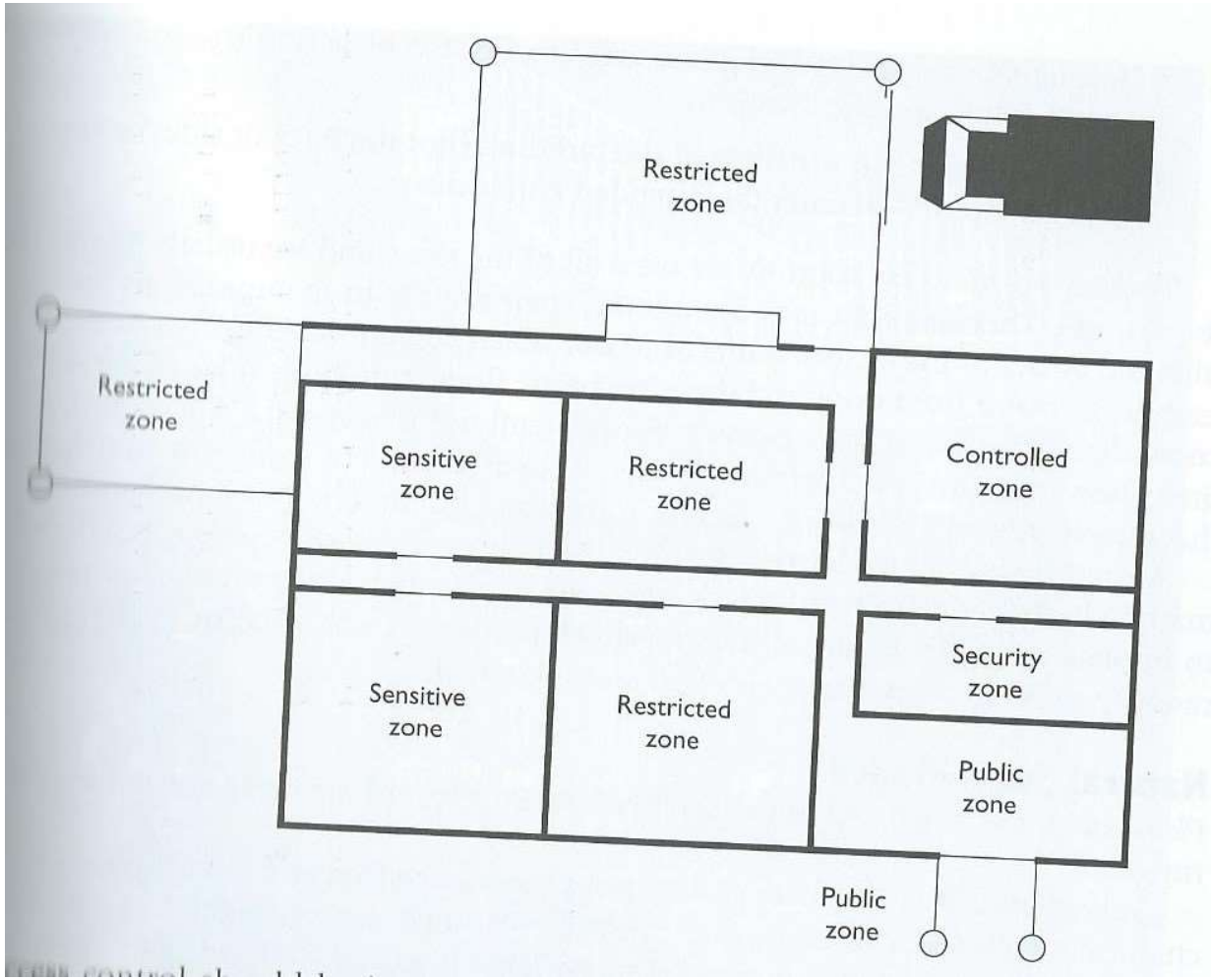
Controles para el acceso natural

- Limitar el número de puntos de entrada
- Forzar a todos los invitados a firmar la entrada y salida del edificio.
- Reducir el número de entrada después de la hora de trabajo o durante el fin de semana.
- Aceras y áreas verdes para guiar al público a la entrada principal.
- Implementar caminos alternativos para proveedores y entregas.

Control de acceso natural



Control de acceso natural



Vigilancia natural

- Puede ser realizada de forma:
  - organizada (ej. con guardias)
  - Mecánica (ej. CCTV)
  - Natural (ej. Áreas despejadas para la vista)

Reforzamiento territorial

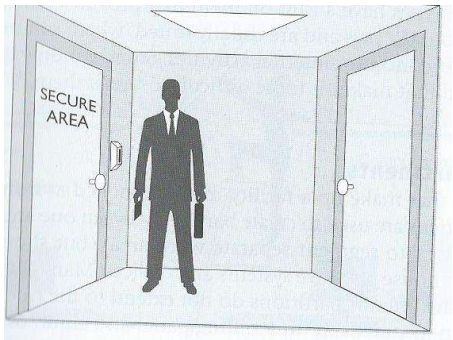
- Por ejemplo
  - Parques
  - Habitaciones de descanso
  - Lugares donde la gente pasee con sus mascotas
  - Actividades de esparcimiento.
- Todos estos controles le dan un sentido de pertenencia a la gente, por lo que la misma gente se da cuenta quien pertenece o quien no y si hay alguna actividad anómala.

Controles ambientales

- Los controles ambientales incluyen una combinación de:
  - controles de acceso físico
  - controles técnicos
  - controles para la seguridad ambiental y de la vida
  - detección y supresión de incendio
  - controles administrativos.

Controles de acceso físico

- Consisten en técnicas y sistemas usados para restringir el acceso a un perímetro de seguridad y proveer una protección en el borde. Estos incluyen:
  - Cercos
  - Conjunto doble de Puertas con seguro (mantraps)
  - Guardia de seguridad
  - Perros guardianes
  - Locks (preseteados, programables, electrónicos)
  - Áreas de almacenaje
  - Tarjetas de acceso
  - Controles de acceso biométricos



Mantraps

Controles técnicos

- Estos incluyen:
  - Vigilancia
  - Detección de intrusos
  - Alarmas
  - de inventario
    - Control físico de PC o laptops
  - de almacenamiento de datos
    - Acceso físico a los medios
    - Reuso del medio y remanencia de los datos

Controles de seguridad ambiental

- Estos controles son necesario para mantener un ambiente seguro y aceptable para los computadores y el personal. Esto controles incluyen:
  - Poder eléctrico
  - HVAC
  - Detección de humo
  - Detección de fuego y supresión

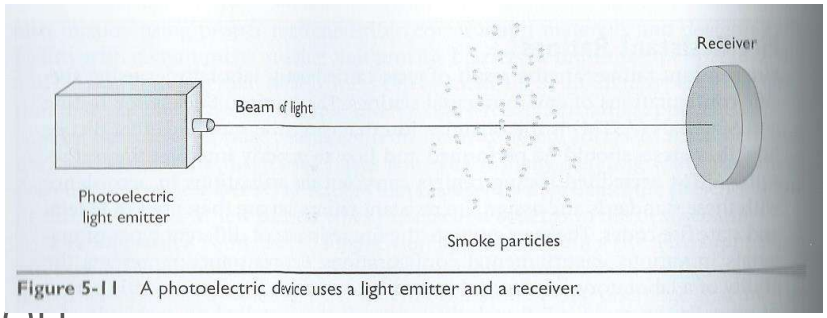
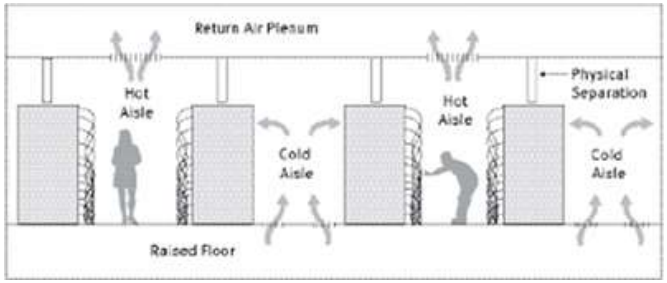


Figure 5-11 A photoelectric device uses a light emitter and a receiver.

HVAC: Heating, Ventilating and Air Conditioning

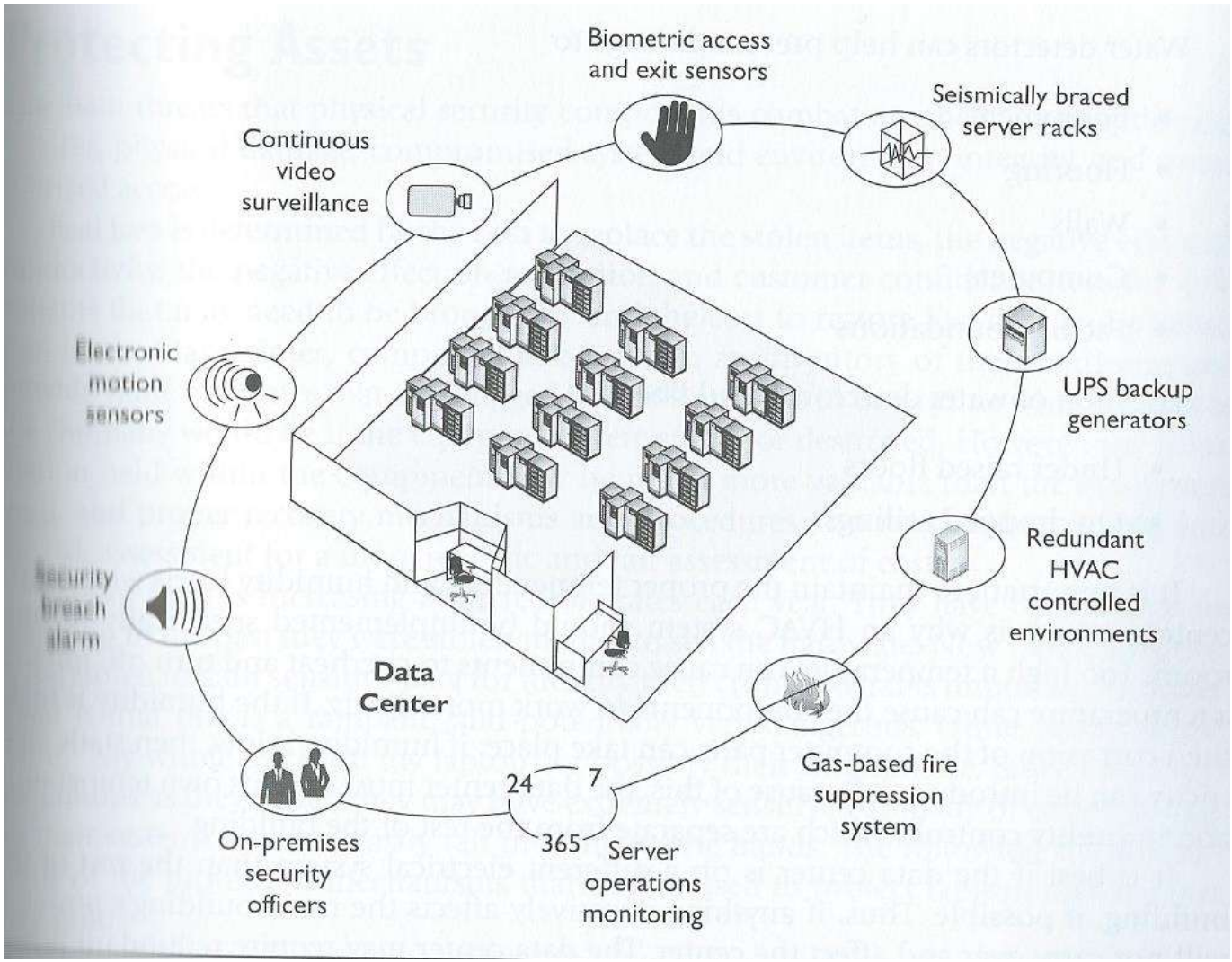
Controles de seguridad ambiental

- Ej: Aire acondicionado, debe ser:
  - Dedicado.
  - Controlable.
  - Electricidad independiente.
  - Controles de apagado de emergencia.
  - Tomas de aire protegidas
  - Monitoreable.



Controles administrativos

- Son los controles que asegura que los controles de acceso físico, controles técnicos, y los controles para la seguridad ambiental y vida, sean adecuadamente implementados y siguen la estrategia general de seguridad física. Estos son:
  - Áreas restringidas
  - Visitantes
  - Privacidad del personal
  - Seguridad
  - Traza de auditorias y logs de accesos
  - Clasificación de activos y control
  - Procedimientos de emergencia
  - Limpieza general
  - Pre y post contratación


Biometric access and exit sensors
Seismically braced server racks
Continuous video surveillance
Electronic motion sensors
UPS backup generators
Redundant HVAC controlled environments
Security breach alarm
Data Center
Gas-based fire suppression system
24
7
365
On-premises security officers
Server operations monitoring

Acercamiento basado en la eficiencia

- Como todos los programas de seguridad, es posible determinar cuanto de beneficioso y efectivo tiene el programa de seguridad física.
- Esto significa que se deben generar métricas para medir la efectividad de las contramedidas.
- Esto permite a la gerencia tomar decisiones de negocio informado, cuando se requiere invertir en la protección de la organización.
- El objetivo es incrementar la efectividad y mitigar el riesgo de la compañía de una manera costo-efectiva.

Algunas métricas

- Número de crímenes exitosos.
- Números de interrupciones exitosas
- Número de crímenes no exitosos
- Número de interrupciones no exitosas.
- Tiempo entre los pasos de detección, evaluación y recuperación.
- Impacto al negocio de las interrupciones.
- Número de alertas de detección falsas positivas
- Tiempo que le toma a un criminal vencer el control
- Tiempo que toma restablecer el ambiente operacional
- Perdida financiera de un crimen exitoso
- Perdida financiera de una interrupción exitosa.

Test de Seguridad Física: Paseo por la oficina

- Comprobar que:
  - Información confidencial o sensitiva de la compañia no se encuentra sobre escritorios o en lugares de acceso público (por ej. impresoras).
  - Las estaciones de trabajo se encuentren desconectadas de la red (logged off) y apagadas.
  - Las oficinas se encuentren cerradas con llave.
  - Las puertas de las salidas de emergencia (escaleras) se encuentren cerradas
  - Escritorios y armarios se encuentren cerrados.
  - Dispositivos de almacenamiento se encuentran debidamente guardados.

Bibliografía

- All in one, CISSP 6th edition, Shon Harris
- CISSP for dummies 4th edition, Lawrence Miler
- IEC/ISO 27002