

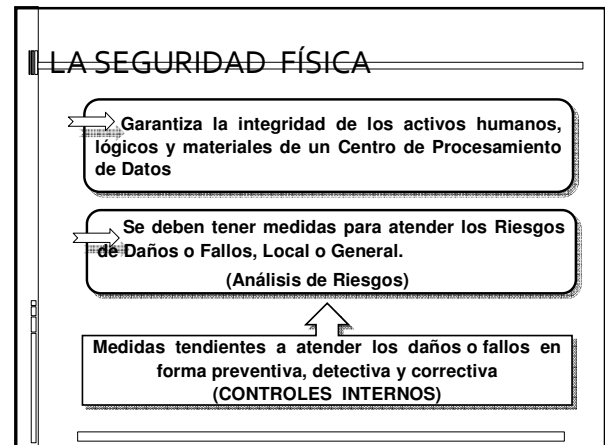


Contenidos

- 1 Seguridad Física
- 2 Auditoría de la Seguridad Física
- 3 Objetivos de la Auditoría
- 4 Áreas de la Seguridad Física
- 5 Medidas a implementar
- 6 Fuentes de la Auditoría
- 7 Técnicas y herramientas de la Auditoría

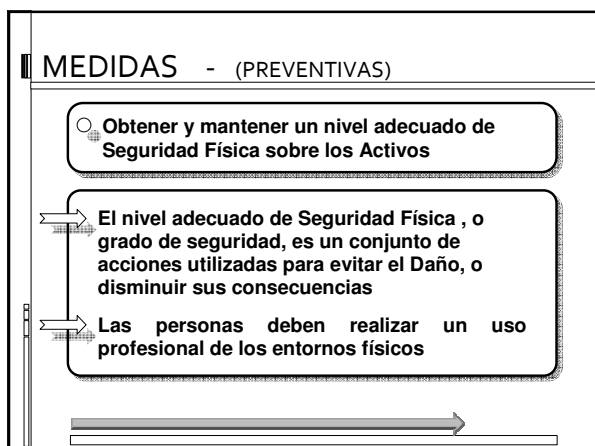
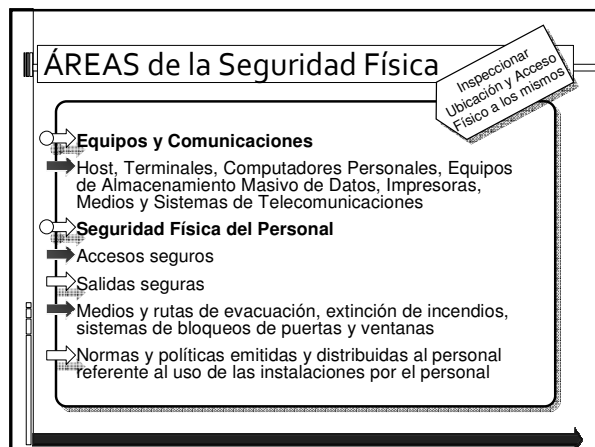
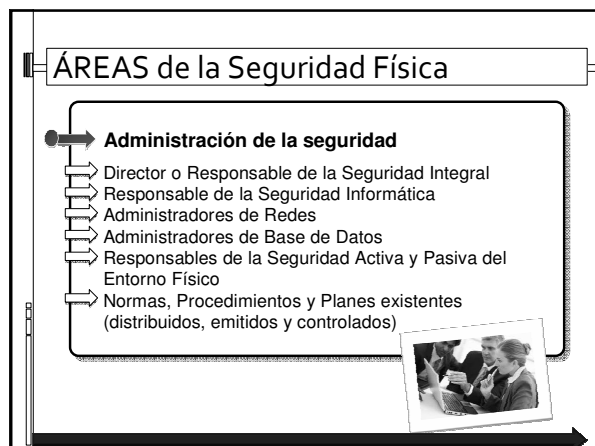
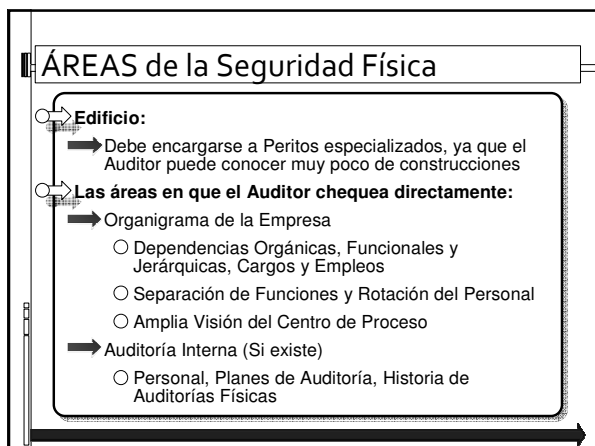
Seguridad FÍSICA

- Mecanismos de prevención y detección destinados a proteger físicamente cualquier recurso del sistema.
- Consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención, detección y contramedidas ante amenazas a los recursos y la información confidencial".



OBJETIVOS de la Auditoría

- Edificio
- Instalaciones
- Equipamiento y Telecomunicaciones
- Datos e Información
- Personas



Ubicación del edificio

- Es el primer paso en un estudio de Seguridad Física.
- **Problema:**
Entorno ya construido, difícilmente modificable y generalmente compartido.
- **Suministro de energía del edificio:**
Parte interna y externa de responsabilidad del proveedor
- **Enlaces de comunicación del edificio:**
Suelen ser públicos y privados. Red telefónica para transporte de voz y datos o las conexiones por Fibra Optica. Redundancia y seguridad física del cableado.

MEDIDAS a Implementar

Buenas Prácticas

- Los edificios de Procesamiento de Datos deben ser discretos y ofrecer un señalamiento mínimo de su propósito
- Las instalaciones claves deben ubicarse en lugares a los cuales NO pueda acceder el público



CPD – Características constructivas

- Tener en cuenta: tipo de datos, número de equipos y tipología (habitación o edificio).
- **Edificios dedicados.**
Zona segura frente a catástrofes naturales.
Rodeado de encofrado (fenómenos ambientales y propiedades ignífugas).
- **Sala de un edificio (Sala cofre).**
Peso del equipamiento (piso o subsuelo).
Falso suelo (cableado y refrigeración).
Falso techo (sistemas de detección y extinción y también refrigeración)
- Accesos exteriores, salidas de emergencia, materiales inflamables.
- Sistema de control de acceso y presencia.

CPD - Climatización

- Aires acondicionados.
- Eliminar calor e inyectar aire en la sala (pasillos fríos).
- Condiciones óptimas de temperatura (17°-19°).
- Humedad: 45%.
- Servidores con disipadores y turbinas en lugar de ventiladores.

CPD – Sistemas de Seguridad

- ✓ **Sistemas Contra incendios**
Material ignífugo.
Detectores, extintores, mangueras, etc.
- ✓ **Sistemas Eléctricos**
Estimar carga a soportar.
Canalizaciones para aislar los cables
Aislamiento contra interferencias, humedades, etc.
Separar líneas eléctricas de las de datos.
Sistema de Alimentación Ininterrumpida (SAI).



CPD – Requisitos

- Disponibilidad y motorización 24*7*365.
- Fiabilidad infalible 99,99% de disponibilidad. No más de 1 hora de fallos al año.
- Seguridad, redundancia y diversificación. Almacenaje de datos, tomas de alimentación eléctrica independientes, control de acceso, etc.
- Control ambiental y prevención de incendios.
- Acceso a Internet y conectividad a redes área extensa.

MEDIDAS a Implementar

Buenas Prácticas




- Los Equipos de Soporte (Fotocopiadoras, Fax, etc.) deben ubicarse adecuadamente
- El Equipamiento debe ubicarse en un sitio que permita Reducir el Riesgo
- El Equipamiento que requiera protección especial debe estar Aislado

MEDIDAS a Implementar

Buenas Prácticas



- Las puertas y ventanas deben bloquearse cuando NO hay Vigilancia
- Implementar Sistema de Detección de Intrusos según estándares reconocidos
- Materiales Peligrosos o Combustibles deben almacenarse en lugares Seguros

MEDIDAS a Implementar

Buenas Prácticas



- Mantener Registro de todas las Fallas y de todo el Mantenimiento Preventivo y Correctivo
- Implementar Controles cuando se Retiran Equipos de la Sede de la Organización para su uso o Mantenimiento

MEDIDAS a Implementar

Buenas Prácticas


- Escritorios Limpios para Proteger Documentos en Papel y Dispositivos de Almacenamiento Removibles
- Políticas de Pantallas Limpias
- Documentos Importantes en Papel y Medios de Información, deben almacenarse Bajo Llave
- Información Sensible debe guardarse en Caja Fuerte o Bóveda a Prueba de Incendio

MEDIDAS a Implementar

Buenas Prácticas

- Las PCs, Terminales e Impresoras NO deben dejarse conectadas cuando están desatendidas
- Proteger Puntos de Recepción y Envío de Correo, Fax y Telex
- Las Fotocopiadoras deben estar bloqueadas fuera del Horario Normal de Trabajo
- La Información Sensible Impresa debe retirarse inmediatamente de la Impresora
- No se debe retirar nada de la Organización sin debida Autorización



MEDIDAS - (DETECTIVAS)

- Ejecutar un Plan de Contingencia adecuado ante un DESASTRE

Desastre: Es cualquier evento , que cuando ocurre, tiene la capacidad de interrumpir el normal proceso de una empresa

Probabilidad BAJA, pero si ocurre puede ser **FATAL**

Los medios necesarios para afrontar el Desastre quedan definidos en el Plan de Recuperación de desastres, que junto con el Centro Alternativo de Proceso de Datos constituyen el PLAN DE CONTINGENCIA



Continúa

PLAN DE CONTINGENCIA

- Establecer Quiénes, y Cómo deben elaborar el plan, implementarlo, probarlo y mantenerlo; qué contemplar y dónde se debe desarrollar el plan.
- **MARCO DEL PLAN:**
 - ¿Debe limitarse a los equipos centrales?
 - ¿Debe incluir los equipos departamentales, PC's y LAN's?
 - ¿Qué procesos son, estratégicamente, más importantes?

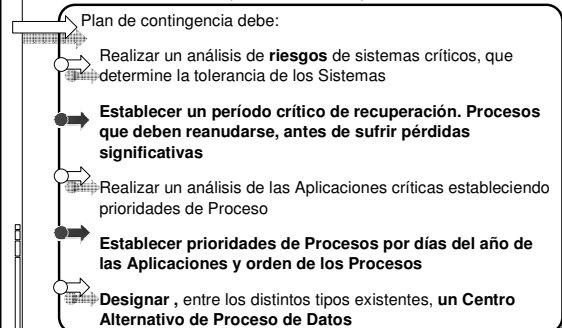
PLAN DE CONTINGENCIA

- **ORGANIZACION:**
 - ¿Quiénes deben componer el equipo de desarrollo del plan?
 - ¿Quién será el responsable de este equipo?
 - ¿Cómo se relacionarán con el resto de la institución?
 - ¿Qué nivel de autonomía tendrá el equipo?
 - ¿A quién reportará?
- **Apoyo institucional. Comunicación e importancia estratégica.**

PLAN DE CONTINGENCIA

- **DETERMINACION DE VULNERABILIDADES:**
 - Obtener información de las consecuencias, que tendría la ocurrencia de un siniestro.
 - Identificación de las aplicaciones críticas. Priorización.
 - Identificación de recursos necesarios para estas aplicaciones.
 - Período máximo de recuperación.
 - Conformidad de todos los involucrados.

MEDIDAS - (DETECTIVAS)



MEDIDAS - (DETECTIVAS)

- ➡ Asegurar la **capacidad de las comunicaciones**
- ➡ Asegurar la capacidad de los servicios de **Backup**
- ➡ Establecer objetivos de recuperación que determinen el período de tiempo (horas, días, semanas) entre la declaración del desastre y el momento en que el **Centro Alternativo** puede Procesar las Aplicaciones críticas

CPD - Centros de Respaldo

- **Sala Fría**
CPD con toda la infraestructura necesaria.
- **Sala Caliente**
CPD con restauración solo de los datos.
- **Mutual Backup**
Acuerdo entre organizaciones para backups mutuos.
- **Centro espejo**
Replicación en tiempo real.

MEDIDAS - (CORRECTIVAS)

- Los **Contratos de Seguros**, compensan en mayor o menor medida las pérdidas, gastos o responsabilidades que se pueden derivar una vez detectado y corregido el fallo.

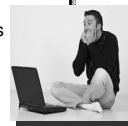
De la gama de seguros pueden darse:

- Centro de Proceso y equipamiento. (Cobertura sobre Daño Físico en el equipo contenido en él)
- Reconstrucción de medios de Software
- Gastos extras (Continuidad de las operaciones; permite compensar la ejecución del Plan de Contingencia)
- Interrupción del negocio (Cubre pérdidas de beneficios netos causados por la caída de Sistemas)
- Documentos y Registros valiosos, por pérdida o Daño Físico

continúa

MEDIDAS - (CORRECTIVAS)

- Errores y omisiones de Profesionales que ocasionen pérdidas
- Cobertura de fidelidad por actos deshonestos o fraudulentos de los Empleados
- Pérdida o daño en el Transporte de Medios
- Contratos con Proveedores y de mantenimiento que aseguren la existencia de repuestos y consumibles así como garantía de fabricación



FUENTES de la Auditoría Física

- Un Centro de Cómputos sigue un modelo organizativo más o menos estándar, según:

- Tipo de Empresa,
- Situación Económica,
- Disponibilidad de Espacio,
- Actitud de la Dirección, etc.



Permiten distinguir que los Centros de Cómputos difieren bastante unos de los otros



FUENTES de la Auditoría Física

Deberían estar accesibles en todo Centro de Cómputos:

- Políticas, Normas y Planes de Seguridad emitidos y distribuidos
- Auditorías anteriores, generales o parciales referidas a Seguridad Física o relacionado a ella
- Contratos de Seguros, de Proveedores y de Mantenimiento
- Actas e Informes de Técnicos y Consultores sobre el Edificio, Electricidad, Aire, etc.
- Informes de Accesos y Visitas
- Informes sobre Pruebas de Evacuación
- Políticas del Personal. Proceso de cancelación de Contratos y Despidos, Rotación en el Trabajo, Contratos Fijos y Temporales
- Inventarios de Soportes (Cintoteca, Back-up, Procedimientos de Archivos, Controles de Salida y Recuperación de Soporte, Control de Copias, etc.)
- Entrevistas con Personal deseado



TÉCNICAS y herramientas del Auditor

- Observación de las **Instalaciones, Sistemas, Cumplimiento de Normas y Procedimientos**, etc. (Tanto de **Espectador** como **Actor**)



TÉCNICAS y herramientas del Auditor

Revisión analítica de:

- Documentación sobre Construcción y Pre-instalaciones
- Documentación sobre Seguridad Física
- Políticas y Normas de Actividad de Sala
- Normas y Procedimientos sobre Seguridad Física de los Datos
- Contratos de Seguros y de Mantenimiento



TÉCNICAS y herramientas del Auditor


- Entrevistas con **Directivos y Personal Fijo o Temporal** (no es interrogatorio)
- Consultas a **Técnicos y Peritos** que formen parte de la plantilla o independientes



TÉCNICAS y herramientas del Auditor

Herramientas:

- Cuaderno de Campo / Grabadora de Audio
- Máquina Fotográfica / Cámara de Video
 - Su uso debe ser discreto y con autorización



PREGUNTAS?

