AUDITORIA DE LA SEGURIDAD FISICA

LA SEGURIDAD FISICA

- Garantiza la integridad de los activos humanos, lógicos y material de un CPD.
- No están claras los límites , dominios y responsabilidades de los tres tipos de seguridad que a los usuarios les interesa: seguridad lógica, seguridad física y seguridad de las comunicaciones
- Se deben tener medidas para atender los riesgos de fallos, local o general.

Medidas…

- Antes
  - Obtener y mantener un nivel adecuado de seguridad física sobre los activos
- Durante
  - Ejecutar un plan de contingencia adecuado
- Después
  - Los contratos de seguros pueden compensar en mayor o menor medida las pérdidas, gastos o responsabilidades que se puedan derivar una vez detectado y corregido el Fallo.

Antes

- El nivel adecuado de seguridad física , o grado de seguridad, es un conjunto de acciones utilizadas para evitar el fallo, o aminorar las consecuencias.
- Es un concepto general , no solo informático, en las que las personas hagan uso particular o profesional de los entornos físicos.

Antes

- Ubicación del edificio
- Ubicación del CPD
- Compartimentación
- Elementos de construcción
- Potencia eléctrica
- Sistemas contra incendios
- Control de accesos
- Selección del personal
- Seguridad de los medios
- Medidas de protección
- Duplicación de los medios

Durante

- Desastre: es cualquier evento , que cuando ocurre, tiene la capacidad de interrumpir e normal proceso de una empresa.
- Se debe contar con los medios para afrontarlo cuando éste ocurra.
- Los medios quedan definidos en el Plan de recuperación de desastres, junto con el centro alternativo de proceso de datos, constituyen el Plan de Contingencia.

Durante

- Plan de contingencia inexcusablemente debe:
  - Realizar un análisis de riesgos de sistemas críticos
  - Establecer un período crítico de recuperación
  - Realizar un análisis de las aplicaciones críticas estableciendo prioridades de proceso.
  - Establecer prioridades de procesos por días del año de las aplicaciones y orden de los procesos
  - Establecer objetivos de recuperación que determinen el período de tiempo (horas, dias , semanas) entre la declaración del desastre y el momento en que el centro alternativo puede procesar las aplicaciones críticas.

Durante

- Designar , entre los distintos tipos existentes, un centro alternativo de proceso de datos.
- Asegurar la capacidad de las comunicaciones
- Asegurar la capacidad de los servicios de Back-up

Después

- De la gama de seguros pueden darse:
  - Centro de proceso y equipamiento
  - Reconstrucción de medios de software
  - Gastos extra (continuidad de las operaciones y permite compensar la ejecución del plan de contingencia)
  - Interrupción del negocio (cubre pérdidas de beneficios netos causados por la caida de sistemas)
  - Documentos y registros valiosos

Después

- Errores y omisiones
- Cobertura de fidelidad
- Transporte de medios
- Contratos con proveedores y de mantenimiento

Areas de la seguridad física

- Edificio :
  - Debe encargarse a peritos especializados
- Las áreas en que el auditor chequea directamente :
  - Organigrama de la empresa
    - Dependencias orgánicas, funcionales y jeráraquicas.
    - Separación de funciones y rotación del personal
    - Da la primera y más amplia visión del Centro de Proceso
  - Auditoría Interna
    - Personal, planes de auditoria, historia de auditorias físicas

Areas de la seguridad física

- Administración de la seguridad
  - Director o responsable de la seguridad integral
  - Responsable de la seguridad informática
  - Administradores de redes
  - Administradores de Base de datos
  - Responsables de la seguridad activa y pasiva del entorno físico
  - Normas, procedimientos y planes existentes
- Centro de proceso de datos e instalaciones
  - Entorno en donde se encuentra el CPD
  - Sala de Host
  - Sala de operadores
  - Sala de impresoras
  - Cámara acorazada
  - Oficinas
  - Almacenes
  - Instalaciones eléctricas
  - Aire acondicionado

Areas de la seguridad física

- Equipos y comunicaciones
  - Host, terminales, computadores personales, equipos de almacenamiento masivo de datos, impresoras, medios y sistemas de telecomunicaciones.
- Seguridad física del personal
  - Accesos seguros
  - Salidas seguras
  - Medios y rutas de evacuación, extinción de incendios, sistemas de bloqueos de puertas y ventanas
  - Normas y políticas emitidas y distribuidas al personal referente al uso de las instalaciones por el personal

Fuentes de la auditoría Física

- Debieran estar accesibles:
  - Políticas , normas y planes de seguridad
  - Auditorías anteriores, generales o parciales
  - Contratos de seguros, de proveedores y de mantenimiento
  - Actas e informes de técnicos y consultores
  - Informes de accesos y visitas
  - Informes sobre pruebas de evacuación
  - Políticas del personal
  - Inventarios de soportes (cintoteca , back-up, procedimientos de archivos, controles de salida y recuperación de soporte, control de copias, etc.)

Técnicas y herramientas del auditor

- Técnicas:
  - Observación de las instalaciones, sistemas, cumplimiento de normas y procedimientos, etc. (tanto de espectador como actor)
  - Revisión analítica de:
    - Documentación sobre construcción y preinstalaciones
    - 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
  - Entrevistas con directivos y personal fijo o temporal (no es interrogatorio)
  - Consultas a técnicos y peritos que formen parte de la plantilla o independientes

- Herramientas:
  - Cuaderno de campo/ grabadora de audio
  - Máquina fotográfica / cámara de video
    - Su uso debe ser discreto y con autorización

Fases de la auditoría física

- Considerando la metodología de ISACA (Information Systems Audit and Control Association)
  - Fase 1 Alcance de la Auditoría
  - Fase 2 Adquisición de Información general
  - Fase 3 Administración y Planificación
  - Fase 4 Plan de auditoria
  - Fase 5 Resultados de las Pruebas
  - Fase 6 Conclusiones y Comentarios
  - Fase 7 Borrador del Informe
  - Fase 8 Discusión con los Responsables de Area
  - Fase 9 Informe Final
    - Informe – anexo al informe – carpeta de evidencias
  - Fase 10 Seguimiento de las modificaciones acordadas