**3.1 Concepto de la seguridad física**

Se evaluaran las protecciones físicas de datos, programas instalaciones, equipos redes y soportes, y por supuesto habrá que considerar a las personas, que estén protegidas y existan medidas de evacuación, alarmas, salidas alternativas, así como que no estén expuestas a riesgos superiores a los considerados admisibles en la entidad e incluso en el sector.

La auditoría física no se debe limitar a comprobar la existencia de los medios físicos, sino también su funcionalidad, racionalidad y seguridad.

La seguridad física existen 3 tipos de seguridad: seguridad lógica. Seguridad física, seguridad de las comunicaciones. La seguridad física garantiza la integridad de los activos humanos, lógicos y materiales contingencia: es la proximidad de algún daño como riesgo de fallo local o general en una relación con la cronología.

**3.2 Áreas a revisar**

**EDIFICIO:**

Debe encargarse a peritos especializados.

* Las áreas en que el auditor chequea directamente:
* Organigrama de la empresa
* Dependencias orgánicas, funcionales y jerárquicas.
* Separación de funciones y rotación del personal
* Da la primera y más amplia visión del centro de proceso
* Auditoria interna.
* Administración de la seguridad
* Director o responsable de la seguridad integral
* Responsable de la seguridad informática
* Administración de redes
* Administradores de base de datos
* Responsables de la seguridad actica y pasiva del entorno físico
* Normas, procedimientos y planes existentes
* Centro de proceso de datos e instalaciones
* Entorno de donde se encuentra el CPD
* Sala de host
* Sala de operadores
* Sala de impresoras
* Cámara acorazada
* Oficinas
* Almacenes
* Instalaciones eléctricas
* Aire acondicionado.
* 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.

**Debieran estar accesibles**

Políticas, normas y planes de seguridad

Auditorias anteriores, generales o parciales

Contratos de seguros, de proveedores y de mantenimiento.

**ANTES**

Obtener y mantener un nivel adecuado de seguridad física sobre los activos.

El nivel adecuado de seguridad física, o grado de seguridad, es un conjunto de acciones utilizadas para evitar el fallo, o aminorar las consecuencias.

* 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**

Ejecutar con un plan de contingencia adecuado.

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 este 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.

DEBE:

* Realizar un análisis de riesgos de sistemas críticos.
* Establecer un periodo 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 periodo de tiempo (horas, días, semanas) entre la declaración del desastre y el momento en que el centro alternativo puede procesar las aplicaciones criticas
* 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**

Los contratos de seguros pueden compensar en mayor o menor medida las perdidas, gastos o responsabilidades que se puedan derivar una vez detectado y corregido el fallo.

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 contigencia)
* Interrupción del negocio (cubre perdidas de beneficios netos causados por la caída de sistemas)
* Documentos y registros valiosos.

**3.3 Evaluación de riesgos**

Retrata de identificar los riesgos, cuantificar su probabilidad de impacto, y analizar medidas que eliminen lo que generalmente no es posible o que disminuya la probabilidad de que o curran los hechos o que mitiguen el impacto.

Para evaluar riesgos hay que considerar, entre otros factores, el tipo de información almacenada procesada y transmitida, la criticidad de las aplicaciones, la tecnología usada, el marco legal aplicable, el sector de entidad, la entidad misma y el momento.

* Observación de las instalaciones, sistemas, cumplimiento de normas y procedimientos, etc
* Revisión analítica de:
* Documentación sobre construccion y preinstalaciones
* Documentación sobre seguridad física
* Políticas y procedimientos sobre seguridad física de los datos
* Contratos seguros y de mantenimiento.
* Entrevistas con directivos y personal fijo o temporal
* Consultas a técnicos y peritos que formen parte de la plantilla o independientes.

**3.4 Fuentes a utilizar**

* Alcance de la auditoria
* Asquisicion de información general
* Administración y planificación
* Plan de auditoria
* Resultados de las pruebas
* Conclusiones y comentarios
* Borrador del informe
* Discusión con los responsables de área
* Informe final
* Seguimiento de las modificaciones acordadas.