CAPÍTULO 8

LA AUDITORÍA FÍSICA

Gabriel Desmonts Basilio

8.1. INTRODUCCIÓN

Lo físico en Informática, hasta ahora, ha tenido una importancia relativa; no en vano se ha visto siempre como algo que soporta lo que, en realidad, es la Informática, y que ocupa un lugar en la mesa.

La UCP (enorme), la pantalla, el teclado, la impresora, cables... y, además, el ratón con su alfombrilla que impiden extender libros y papeles sobre un espacio que, incomprensiblemente, por grande que sea, no existe.

Pero lo físico en Informática no se reduce únicamente a lo expuesto, esto es: dar un soporte tangible, un continente o vehículo a lo etéreo del software, verdadera esencia informática. Todo cuanto rodea o se incluye en el computador, también este mismo, son lo físico como tal, así como otros conceptos o virtualidades que, de una u otra forma, influyen o toman su razón de ser en el Entorno Físico del computador como generalidad o en el del CPD como Unidad Física Informática.

Si se ha dicho que lo físico es algo tangible que proporciona un continente, medio o vehículo y que, además, acoge al CPD dentro de su entorno, una vez conseguido y establecido debería dejar de preocupar. El paso siguiente es asegurarse de que va a seguir dando servicio siempre que se le necesite y de una manera segura ya que, como en toda actividad, se mezcla lo físico con lo funcional y con lo humano.

La Auditoría es el medio que va a proporcionar la evidencia o no de la Seguridad Física en el ámbito en el que se va a desarrollar la labor profesional. Es por tanto, necesario asumir que la Auditoría Física no se debe limitar a comprobar la existencia

de los medios físicos, sino también su funcionalidad, racionalidad y seguridad, palabra esta última que puede resumir o incluir a las anteriores y llevar a un subtítulo de este capítulo que prolongue el ya establecido de Auditoría Física con el de *Auditoría de la Seguridad Física.*

8.2. LA SEGURIDAD FÍSICA

No están muy claras las fronteras que delimitan, si es que lo hacen, los dominios y responsabilidades de los tres tipos de seguridad que a los usuarios de la Informática deben interesar: seguridad lógica, seguridad física y seguridad de las Comunicaciones. Quizá fuera más práctico aunarlas y obtener una seguridad integral, aunque hay que reconocer las diferencias que, evidentemente, existen entre *soft, hard, hard-soft, hard* que soporta al *soft* y *soft* que mueve al *hard.*

La seguridad física garantiza la integridad de los activos humanos, lógicos y materiales de un CPD. Si se entiende la contingencia o proximidad de un daño como la definición de Riesgo de Fallo, local o general, tres serían las medidas a preparar para ser utilizadas en relación con la cronología del fallo:

8.2.1. 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, en su caso, aminorar las consecuencias que de él se puedan derivar.

Es un concepto general aplicable a cualquier actividad, no sólo informática, en la que las personas hagan uso particular o profesional de entornos físicos.

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

8.2.2. Durante

Ejecutar un Plan de Contingencia adecuado.

En general, *desastre* es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso de una empresa.

La probabilidad de que ocurra un desastre es muy baja, aunque, si se diera, el impacto podría ser tan grande que resultara fatal para la organización. Como, por otra parte, no es corriente que un negocio responda por sí mismo ante un acontecimiento como el que se comenta, se deduce la necesidad de contar con los medios necesarios para afrontarlo. Estos medios quedan definidos en el Plan de Recuperación de Desastres que, junto con el Centro Alternativo de Proceso de Datos, constituye el *Plan de Contingencia* que coordina las necesidades del negocio y las operaciones de recuperación del mismo.

El Plan de Contingencia inexcusablemente debe:

- Realizar un Análisis de Riesgos de Sistemas Críticos que determine la Tolerancia de los Sistemas.
- Establecer un Período Crítico de Recuperación en el cual los procesos deben ser reanudados antes de sufrir pérdidas significativas o irrecuperables.
- Realizar un Análisis de Aplicaciones Críticas por el que se establecerán las Prioridades de Proceso.
- Determinar las Prioridades de Proceso, por días del año, que indiquen cuáles son las Aplicaciones y Sistemas Críticos en el momento de ocurrir el desastre y el orden de proceso correcto.
- Establecer Objetivos de Recuperación que determinen el período de tiempo (horas, días, semanas) entre la declaración de Desastre y el momento en que el Centro Alternativo puede procesar las Aplicaciones Críticas.
- Designar, entre los distintos tipos existentes, un Centro Alternativo de Proceso de Datos.
- Asegurar la Capacidad de las Comunicaciones y
- Asegurar la Capacidad de los Servicios de Back-up.

8.2.3. Después

Los Contratos de Seguros vienen a compensar, en mayor o menor medida, las pérdidas, gastos o responsabilidades que se pueden derivar para el CPD una vez detectado y corregido el Fallo.

De entre la gama de seguros existentes, se pueden señalar:

- *Centros de proceso y equipamiento*: Se contrata cobertura sobre daño físico en el CPD y el equipo contenido en él.

- *Reconstrucción de medios software*: Cubre el daño producido sobre medios *soft* tanto los que son propiedad del tomador del seguro como aquellos que constituyen su responsabilidad.

- *Gastos extra*: Cubre los gastos extra que se derivan de la continuidad de las operaciones tras un *desastre* o daño en el CPD. Es suficiente para compensar los costos de ejecución del Plan de Contingencia.

- *Interrupción del negocio*: Cubre las pérdidas de beneficios netos causadas por las caídas de los medios informáticos o por la suspensión de las operaciones.

- *Documentos y registros valiosos*: Se contrata para obtener una compensación en valor metálico real por la pérdida o daño físico sobre documentos y registros valiosos no amparados por el seguro de Reconstrucción de Medios Software.

- *Errores y omisiones*: Proporciona protección legal ante la responsabilidad en que pudiera incurrir un profesional que cometiera un acto, error u omisión que ocasione una pérdida financiera a un cliente.

- *Cobertura de fidelidad*: Cubre las pérdidas derivadas de actos deshonestos o fraudulentos cometidos por empleados.

- *Transporte de medios*: Proporciona cobertura ante pérdidas o daños a los medios transportados.

- *Contratos con proveedores y de mantenimiento*: Proveedores o fabricantes que aseguren la existencia de repuestos y consumibles, así como garantías de fabricación.

Contratos de mantenimiento que garanticen la asistencia técnica a los equipos e instalaciones una vez extinguidas las garantías de fabricación.

No son realmente Seguros, ya que:

- Los primeros se ubicarían en Nivel adecuado de Seguridad Física (el **antes**).
- Los segundos pueden localizarse tanto en el Nivel adecuado (el **antes**) como en el Plan (el **durante**).

No obstante, dada su forma y su control administrativo, se les puede considerar como Seguros.

8.3. ÁREAS DE LA SEGURIDAD FÍSICA

Se ha expuesto, hasta el momento, un estudio de las tres medidas a preparar para ser utilizadas según el momento del Fallo: riesgo de que se produzca, si se está produciendo y cuando ha pasado. Todo ello partiendo, como primer paso, de la ubicación del edificio y las circunstancias externas e internas que le afectan.

Nada se ha dicho del edificio en sí mismo: ¿sería capaz el Auditor Informático de revisar la construcción y el estado actual de su infraestructura con sus defectos, vicios y posibles enfermedades? Más aún: ¿es capaz de diagnosticar en este tema? Evidentemente, como tal auditor, carece de la capacidad y preparación necesarias para ello. Por tanto, debe considerarse al edificio como la primera de las áreas a tener en cuenta en una Auditoría Física y prever para ella el auxilio de Peritos independientes que den respuestas a las preguntas a plantear durante la Fase 2 del Procedimiento de Auditoría *Adquisición de Información General* y certificaciones que puedan ser incluidas como pruebas, en uno o en otro sentido, en la Fase 9 *Informe Final* tras la *Discusión con los Responsables* si hubiera lugar.

Las áreas en las que el Auditor ha de interesarse personalmente, una vez que la parte del edificio ha sido encargada al juicio del Perito, tendrán relación directa con el hecho informático, siempre considerando el aspecto físico de la seguridad, y que serán tales como:

Organigrama de la empresa

Por él se conocerán las dependencias orgánicas, funcionales y jerárquicas de los departamentos y de los distintos cargos y empleos del personal pudiendo analizar, con

ayuda de documentación histórica, las apropiadas Separación de Funciones y Rotación en el Trabajo.

Da la primera y más amplia visión de conjunto del Centro de Proceso.

Auditoría interna

Departamento independiente o subordinado al de Auditoría Financiera, si existe, y colaborador de éste en cualquier caso, debe guardar las auditorías pasadas, las Normas, Procedimientos y Planes que sobre la Seguridad Física y su Auditoría hayan emitido y distribuido la Autoridad competente dentro de la Empresa.

Administración de la seguridad

Vista desde una perspectiva general que ampare las funciones, dependencias, cargos y responsabilidades de los distintos componentes:

- Director o Responsable de la Seguridad Integral.
- Responsable de la Seguridad Informática.
- Administradores de Redes.
- Administradores de Bases de Datos.
- Responsables de la Seguridad activa y pasiva del Entorno físico.

Normas, Procedimientos y Planes que, desde su propia responsabilidad hayan emitido, distribuido y controlado el departamento.

Centro de proceso de datos e instalaciones

Entorno en el que se encuentra incluso el CPD como elemento físico y en el que debe realizar su función informática.

Las instalaciones son elementos accesorios que deben ayudar a la realización de la mencionada función informática y, a la vez, proporcionar seguridad a las personas, al soft y a los materiales.

- Sala del Host.
- Sala de Operadores.
- Sala de Impresoras.
- Cámara Acorazada.
- Oficinas.

- Almacenes.
- Sala de aparamenta eléctrica.
- Sala de Aire Acondicionado.
- Área de descanso y servicios...

Equipos y comunicaciones

Son los elementos principales del CPD: Host, terminales, computadores personales, equipos de almacenamiento masivo de datos, impresoras, medios y sistemas de telecomunicaciones...

El Auditor debe inspeccionar su ubicación dentro del CPD así como el Control de Acceso a los mismos como elementos restringidos.

Computadores personales

Especialmente cuando están en red, son elementos muy potentes e indiscretos que pueden acceder a prácticamente cualquier lugar donde se encuentren los Datos *(primer objetivo de toda seguridad)*, por lo que merecerán especial atención tanto desde el punto de vista de acceso a los mismos como a la adquisición de copias *(hard y soft)* no autorizadas. Es especialmente delicada su conexión a los medios de telecomunicaciones.

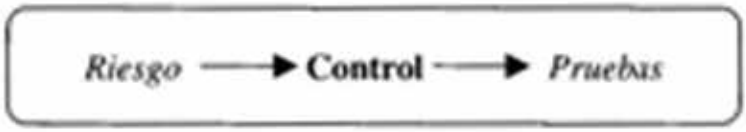
Seguridad física del personal

Accesos y salidas seguras así como medios y rutas de evacuación, extinción de incendios y medios utilizados para ello (agua en lugares con conducciones y aparatos eléctricos, gases asfixiantes...), sistemas de bloqueo de puertas y ventanas, zonas de descanso y de servicios...

Normas y Políticas emitidas y distribuidas por la Dirección referentes al uso de las instalaciones por el personal.

8.4. DEFINICIÓN DE AUDITORÍA FÍSICA

La Auditoría Física, interna o externa, no es sino una auditoría parcial, por lo que no difiere de la auditoría general más que en el Alcance de la misma.



8.5. FUENTES DE LA AUDITORÍA FÍSICA

Ya se ha comentado, brevemente en los párrafos anteriores, cuáles pueden ser algunas de las Fuentes donde la Auditoría va a encontrar la información necesaria para organizar y desarrollar la Fase 4 del Procedimiento o Ciclo de Vida de la Auditoría *"Plan de Auditoría"* que le llevará a realizar las pertinentes Pruebas de Cumplimiento y Sustantivas.

Un CPD, en esencia, sigue un modelo organizativo más o menos estándar, aunque debido a diferentes causas, como puede ser el tipo de empresa a la que pertenece, situación económica, disponibilidades de espacio, actitud de la Dirección, etc. hacen que, en realidad, los CPD's difieran bastante los unos de los otros.

Se señalan a continuación algunas Fuentes que deben estar accesibles en todo Centro de Proceso de Datos.

- *Políticas, Normas y Planes* sobre Seguridad emitidos y distribuidos tanto por la Dirección de la empresa en términos generales como por el Departamento de Seguridad siguiendo un enfoque más detallado.

- *Auditorías anteriores,* generales y parciales, referentes a la Seguridad Física o a cualquier otro tipo de auditoría que, de una u otra manera, esté relacionada con la Seguridad Física.

- *Contratos de Seguros, de Proveedores y de Mantenimiento.*

- *Entrevistas* con el personal de seguridad, personal informático y de otras actividades, responsables de seguridad de otras empresas dentro del edificio y de la seguridad general del mismo, personal contratado para la limpieza y mantenimiento de locales, etc.

- *Actas e Informes* de técnicos y consultores. Peritos que diagnostiquen el estado físico del edificio, electricistas, fontaneros, técnicos del aire acondicionado, especialistas en electrónica que informen sobre la calidad y estado de operatividad de los sistemas de seguridad y alarma, agencias de seguridad que proporcionan a los Vigilantes jurados, bomberos, etc.

- *Plan de Contingencia y valoración de las Pruebas.*

- *Informes sobre accesos y visitas.* Existencia de un sistema de control de entradas y salidas diferenciando entre áreas Perimetral, Interna y Restringida.

  Informes sobre pruebas de evacuación ante diferentes tipos de amenaza: incendio, catástrofe natural, terrorismo, etc.

  Informes sobre evacuaciones reales.

- *Políticas de Personal.* Revisión de antecedentes personales y laborales, procedimientos de cancelación de contratos y despidos, rotación en el trabajo, planificación y distribución de tareas, contratos fijos y temporales.

- *Inventarios de Soportes* (papel y magnéticos): cintoteca, back-up, procedimientos de archivo, controles de salida y recuperación de soportes, control de copias, etc.

8.6. OBJETIVOS DE LA AUDITORÍA FÍSICA

Más arriba, en Áreas de la Seguridad Física párrafo Computadores Personales, se decía que los Datos son el primer objetivo de toda seguridad. Bien entendido que hacía referencia a toda seguridad informática, la Seguridad Física es más amplia y alcanza otros conceptos entre los que puede haber alguno que supere en importancia a los propios datos.

Sin otro ánimo más que el mero orden basado en una lógica *"de fuera adentro"*, quedan indicados estos Objetivos como sigue:

- Edificio.
- Instalaciones.
- Equipamiento y telecomunicaciones.
- Datos.
- Personas.

8.7. TÉCNICAS Y HERRAMIENTAS DEL AUDITOR

Como se verá, no se diferencian de las técnicas y herramientas básicas de toda auditoría y, como en ellas, su fin es obtener la Evidencia física.

Técnicas:

- *Observación* de las instalaciones, sistemas, cumplimiento de Normas y Procedimientos, etc. no sólo como espectador sino también como actor, comprobando por sí mismo el perfecto funcionamiento y utilización de los conceptos anteriores.

- 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, que no dé la sensación de interrogatorio para vencer el natural recelo que el auditor suele despertar en los empleados.

- *Consultas* a técnicos y peritos que formen parte de la plantilla o independientes contratados.

Herramientas:

- *Cuaderno de campo / grabadora de audio*
- *Máquina fotográfica / cámara de vídeo*

Su uso debe ser discreto y siempre con el consentimiento del personal si éste va a quedar identificado en cualquiera de las máquinas.

8.8. RESPONSABILIDADES DE LOS AUDITORES

El Auditor Informático, en especial el Interno, no debe desarrollar su actividad como una mera *función policial* dando la impresión a los usuarios informáticos y al resto de empleados de que se encuentran permanentemente vigilados. Esto crea un ambiente tenso y desagradable que en nada favorece ni a las relaciones personales ni al buen desarrollo del trabajo.

El auditor debe esforzarse más en dar una imagen de colaborador que intenta ayudar que en la de fiscalizador o caza-infractores. Para ello es necesario que en las Normas y Procedimientos emitidos por la Dirección figuren las funciones y responsabilidades de los auditores y que ambas sean distribuidas y conocidas por toda la plantilla de la empresa.

Dentro del campo de responsabilidades de los auditores, las referentes a Seguridad Física, quedan establecidas las siguientes para cada tipo de auditor:

Auditor informático interno

- Revisar los controles relativos a Seguridad Física.
- Revisar el cumplimiento de los Procedimientos.
- Evaluar Riesgos.
- Participar sin perder independencia en:
  - Selección, adquisición e implantación de equipos y materiales.
  - Planes de Seguridad y de Contingencia, seguimiento, actualización, mantenimiento y pruebas de los mismos.
- Revisión del cumplimiento de las Políticas y Normas sobre Seguridad Física así como de las funciones de los distintos Responsables y Administradores de Seguridad.
- Efectuar auditorías programadas e imprevistas.
- Emitir informes y efectuar el seguimiento de las recomendaciones.

Auditor informática externo

- Revisar las funciones de los auditores internos.
- Mismas responsabilidades que los auditores internos.
- Revisar los Planes de Seguridad y Contingencia. Efectuar Pruebas.
- Emitir informes y recomendaciones.

8.9. FASES DE LA AUDITORÍA FÍSICA

Siguiendo la Metodología EDPAA y sin perjuicio de alguna pequeña diferencia, más que nada en el orden o el ámbito de las fases, el Ciclo de Vida quedaría:

Fase 1: Alcance de la Auditoría
Fase 2: Adquisición de Información General
Fase 3: Administración y Planificación
Fase 4: Plan de Auditoría
Fase 5: Resultado de las Pruebas
Fase 6: Conclusiones y Comentarios
Fase 7: Borrador del Informe
Fase 8: Discusión con los Responsables de Área
Fase 9: Informe Final

- Informe
- Anexo al Informe
- Carpeta de Evidencias

Fase10: Seguimiento de las Modificaciones acordadas.

8.10. DESARROLLO DE LAS FASES DE LA AUDITORÍA FÍSICA

Resulta clara la práctica identidad entre el Ciclo de Vida de la Auditoría Física con cualquier otro de una auditoría diferente.

Con la intención de ofrecer algo práctico dentro de tanta teoría, se expone a continuación el desarrollo de la Fase 2 *Adquisición de Información* referente a un Plan de Contingencia, siguiendo la técnica del *check-list* para un mejor entendimiento de los conceptos.

La lista es, naturalmente, orientativa y en ningún caso se puede considerar completa.

Auditoría del plan de contingencia

Fase 2 Adquisición de Información

Acuerdo de Empresa para el Plan de Contingencia

- ¿Hay algún acuerdo oral o escrito por parte de la Dirección?
- ¿Ha emitido y distribuido la empresa Políticas o Normas dirigidas al Plan de Contingencia?
- ¿Qué persona o departamento tiene la responsabilidad del Plan?
- ¿Están las responsabilidades de Planeamiento bien definidas, difundidas y entendidas por todo el personal?
- ¿Se mantiene una estrategia corporativa en el Plan? Todos los departamentos deben cooperar en el Plan desde su propia especialidad o responsabilidad.

- ¿Incluyen los presupuestos empresariales fondos destinados al desarrollo y mantenimiento del Plan de Contingencia?

Acuerdo de un Proceso Alternativo

- ¿Está el Acuerdo obligado e impuesto legalmente cuando se produce un desastre?
- ¿Es compatible el equipamiento del Proceso de Datos en el Centro Alternativo con el equipamiento en el CPD?
- ¿Proporciona el Centro Alternativo suficiente capacidad?
- ¿Cuándo fue la última vez que se probó el Centro Alternativo?
- ¿Cuáles fueron los objetivos y el alcance de la prueba?
- ¿Cuáles fueron los resultados de la prueba?, ¿quedaron los resultados bien documentados?
- ¿Han sido implementadas acciones correctivas o están previstas para una futura implementación?
- ¿Está prevista una próxima prueba de uso del Centro Alternativo?
- ¿Utiliza la empresa algún equipamiento de proceso que pueda no estar soportado por el Centro Alternativo?

Protección de Datos

- ¿Tiene la empresa un Centro Externo para el almacenamiento de los *back-up?*
- ¿Se ha realizado alguna vez una auditoría de las cintas y discos almacenados en el Centro Back-up Externo?
- ¿Cuál es el Procedimiento de Acceso al Centro Externo para la obtención de los back-up en el caso de un desastre?
- ¿Cuál es el Procedimiento de Transporte de los back-up desde el Centro Externo al Centro de Proceso Alternativo?

- ¿Cuál es la estrategia para la Restauración de programas?, ¿serán almacenadas las aplicaciones simultáneamente o en fases basadas en prioridades?
- ¿Ha sido asignada prioridad de restauración a cada aplicación?
- ¿Han sido identificados todos los archivos críticos?
- ¿Se han creado los back-up de los archivos críticos según una base metódica?
- ¿Existe un mínimo de tres ciclos de copias de back-up en el Centro Externo?
- ¿Existen copias actualizadas de los Informes del Sistema de Gestión de Cintas almacenadas en el Centro Back-up Externo?

Manual del Plan de Contingencia

- ¿Cómo está estructurado el Plan?
- ¿Es fácil de seguir el Plan en el caso de un desastre?
- ¿Indica el Plan quién es el responsable de desarrollar tareas específicas?
- ¿Cómo se activa el Plan ante un desastre?
- ¿Cómo están contenidos estos procedimientos de activación en los procedimientos de emergencia normales de la empresa?
- ¿Han sido probados estos procedimientos en un test de desastre simulado?
- ¿Contiene el Plan procedimientos que fijen los daños en las etapas iniciales de las Operaciones de Recuperación?
- ¿Incluye el Plan procedimientos para trasladar el proceso desde el Centro Alternativo al Centro Restaurado o Nuevo?
- ¿Contiene el Plan listados del Inventario del proceso de datos y *hard* de comunicaciones, software, formularios preimpresos y stock de papel y accesorios?
- ¿Están actualizados los listines telefónicos del personal de Recuperación así como empleados del Proceso de Datos, alta dirección, usuarios finales y vendedores y suministradores?

- ¿Cómo está mantenido el Plan?
- ¿Quién es el responsable de actualizar el Plan?
- ¿Se mantiene el *Log* de distribución del Plan?
- ¿Cuándo fue actualizado el Plan por última vez?
- ¿Existe una copia del Plan en el Centro Externo de *Back-up?*

8.11. LECTURAS RECOMENDADAS

Thomas, A. J. y Douglas, I. J. *Auditoría Informática.* Paraninfo, Madrid, 1987.
Contingency Planning. Auerbach Publishers.

8.12. CUESTIONES DE REPASO

1. Diferencie entre seguridad lógica, seguridad física y seguridad de las comunicaciones, poniendo varios ejemplos de cada tipo.
2. Explique el concepto de "nivel adecuado de seguridad física".
3. ¿Cómo definiría lo que constituye un "desastre"?
4. ¿Qué tipos de seguros existen?
5. ¿Qué medios de extinción de fuego conoce?
6. ¿Por qué es importante la existencia de un sistema de control de entradas y salidas?
7. ¿Qué técnicas cree que son las más adecuadas para la auditoría física?
8. ¿Cuáles suelen ser las responsabilidades del auditor informático interno respecto a la auditoría física?
9. ¿Qué aspectos considera más importantes a la hora de auditar el plan de contingencia desde el punto de vista de la auditoría física?
10. ¿Qué riesgos habría que controlar en el centro de proceso alternativo?