



Seguridad de los Sistemas Informáticos

Tema 4. Seguridad física

Objetivos de aprendizaje²



- Conocer los peligros asociados al acceso físico al sistema informático.
- Ser capaz de prever los peligros que puede tener una instalación informática desde el punto de vista de su integridad física.
- Ser capaz de diseñar a alto nivel la instalación física de un sistema informático de manera que cumpla con unos requisitos mínimos de seguridad.



La **seguridad física** hace referencia a:

- a) La seguridad del **entorno** donde están ubicados los activos de la organización (y que pueden comprometer su propia seguridad): edificio, instalaciones eléctricas, de gas, de agua, de aire acondicionado, puntos de acceso (puertas, ventanas, ...)
- b) La seguridad del **equipamiento físico** de un sistema informático: ordenadores, cableado eléctrico y de red, dispositivos de red, ...
- c) La seguridad del **personal** encargado de los sistemas o de la seguridad de los mismos (administradores, técnicos, personal de seguridad, ...)

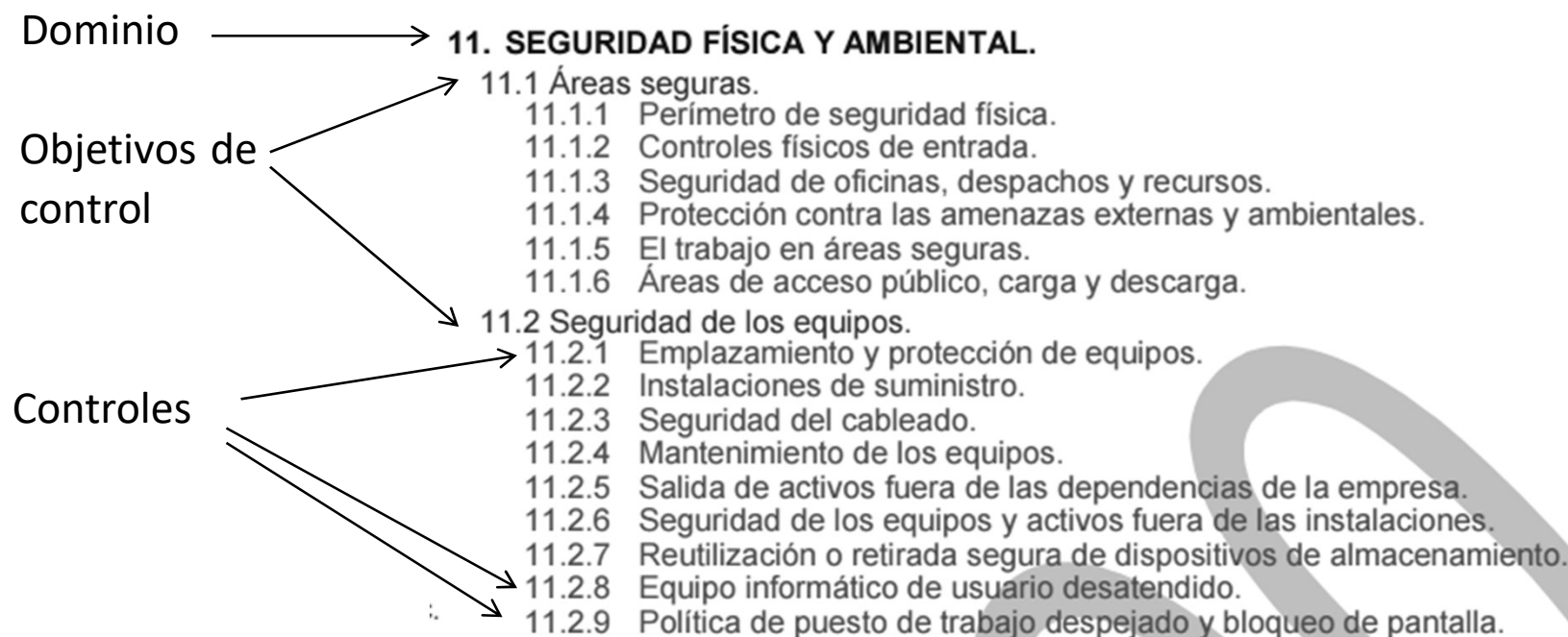
Se trata en general de evitar daños e interferencias contra los locales y la información de la organización así como accesos no autorizados.



Estos posibles fallos han de localizarse:

- En el funcionamiento normal de la organización.
- En situaciones extraordinarias.
- Ante intrusos.
- Ante ataques intencionados.

Recordemos los controles de ISO 27002



Y la metodología OSSTMM

OSSTMM 3 – The Open Source Security Testing Methodology Manual

8.5 Access Verification

Tests for the enumeration of access points to interact with the targets and assets within the scope. While access to walls and fences bordering property outside of the scope is a real scenario and one often used in an attack, this audit is limited to scope-only interaction to protect the property rights of third parties.

8.5.1 Enumeration

- (a) Map and explore the navigable of terrain, barriers, and obstacles into the scope to reach the targets and assets. Document all methods used and the results of those methods.
- (b) Map and verify all access points that allow stealthy or unmonitored, direct (3 seconds or less time on target) interaction with the target.
- (c) Verify the size and navigable of public and private access points and all paths to target.

8.5.2 Authentication

- (a) Enumerate and test for inadequacies which privileges are required to access, the process of obtaining those privileges, and assure that only identifiable, authorized, intended parties are provided access.
- (b) Verify the process of authenticating which items may be taken into the scope by both authorized and unauthorized personnel.
- (c) Verify the process of authenticating which items may be taken out of the scope by both authorized and unauthorized personnel.
- (d) Verify the process of recording access and which items were entered and removed.



Además de...

- http://www.cni.es/comun/recursos/descargas/NS-03_Seguridad_Fisica.pdf
- https://boe.es/diario_boe/txt.php?id=BOE-A-2011-8849



Seguridad física del Entorno

1. Accesos físicos
2. Acceso al CPD
3. Amenazas externas y ambientales
4. Suministro de energía
5. Comunicaciones
6. Seguridad en despachos
7. Trabajo en áreas seguras
8. Warchalking



- Relativo a la Seguridad física, el primer elemento a considerar es el “contenedor” de los equipos: el **edificio** que los alberga.
- Para verificar la seguridad física de una organización es necesario contar con planos actualizados del edificio.

5.2 Seguridad Física

Contempla el nivel de seguridad física alcanzado en las instalaciones que albergan la Sala de Máquinas objeto de estudio.

5.2.1 Ubicación

Las instalaciones del Centro se encuentran en el Edificio de Ciencias del Campus de Llamaquique, situado en la Calle Calvo Sotelo s/n, repartidas por las plantas del sótano, bajo, primera, segunda y tercera (incluyendo bajocubierta). Todas ellas comparten instalaciones con aulas de formación y despachos del profesorado.

En la planta sótano se encuentra la acometida de suministro y las calderas del sistema de calefacción, así como el cuadro central de activación de dispositivos de seguridad (aspersores, circuitos hidráulicos, eléctricos, etc.). Esta planta dispone de dos accesos a la calle, uno de ellos es la salida de emergencia y el otro el patio de acceso a la vivienda del bedel. La entrada principal al edificio se encuentra en la planta baja, interceptada por un doble cierre de verja de hierro y puertas de cristal, tras las que se encuentra situada la cabina de Conserjería.

Diagnóstico de Seguridad de los Sistemas de Información. PFC cód. DMKPC-0737. EUITIO

Entorno - Accesos físicos (I)

10



- Debe realizarse un inventario de todos los posibles accesos.
- Es necesario comprobar todos los accesos al edificio para que los usuarios no autorizados no puedan entrar en él.
 - Tanto a través de medios habituales: puertas de acceso al edificio, puertas de servicio, portón del garaje...
 - Como de otros medios: ventanas, claraboyas, conductos de servicio o ventilación, ...
- Se propondrán todas aquellas medidas (rejas, cerraduras, detectores, cámaras, ...) que se estimen necesarias.

Entorno - Accesos físicos (II)

☑ *Enumerar las áreas con control de acceso.*

Todos los edificios de **EUITIO** (incluyendo el **Aulario de Geológicas** y la **Facultad de Magisterio**) disponen de control de acceso al edificio mediante cabinas.

Dentro del **Edificio de Ciencias**, el acceso a los laboratorios, aulas, despachos y secretaría se controla mediante cerradura. Las llaves son almacenadas por el responsable del despacho, guardando siempre el bedel en la garita de la entrada una copia de todas las llaves del edificio. La garita está cerrada, a su vez, por una llave que sólo tiene el bedel.

☑ *Examinar los tipos de dispositivos de control e acceso.*

Los accesos a las áreas restringidas se controlan mediante cerradura ordinaria. Los accesos desde el exterior se controlan mediante rejas y portales de hierro en las puertas y ventanas de la planta baja.

☑ *Examinar los tipos de alarmas.*

Todas las alarmas han sido desactivadas debido al elevado número de incidentes diarios que provocaban los alumnos.

☑ *Determinar el nivel de complejidad de los dispositivos de control de acceso.*

Las cerraduras y las llaves no son de seguridad. Las puertas que cierran el acceso a las áreas restringidas dentro de los edificios no son blindadas, ni los marcos tampoco.

Las rejas que protegen las ventanas de la planta baja son fijas. No obstante, algunas ventanas de la primera planta son relativamente sencillas de alcanzar y no disponen de ningún medio de disuasión ante ataques intrusivos.

Diagnóstico de Seguridad de los Sistemas de Información. PFC cód. DMKPC-0737. EUITIO

Entorno - Acceso al CPD

12

- Independientemente de las políticas y medidas de acceso aplicadas al edificio, el acceso al CPD debe ser estudiado y protegido con especial cuidado.
- Los accesos deben ser controlados, y sólo podrán acceder los usuarios autorizados (cerraduras electrónicas con código de acceso, guardias de seguridad, ...).
- Todos los accesos (incluido personal de limpieza, mantenimiento, etc.) deben estar autorizados y seguir el procedimiento establecido.
- Debe estar convenientemente aislado a través de paredes y puertas suficientemente sólidas (no mediante mamparas o similares).
- No debe tener otros accesos que los habituales (ventanas, conductos).



Grado en Ingeniería Informática del Software
Seguridad de Sistemas Informáticos

Entorno - Amenazas externas y Ambientales (I)

- El diseño y construcción del edificio debe estar realizado para minimizar los efectos de posibles desastres que puedan darse en el entorno donde se ubique. En zonas sísmicas deberá prestarse especial atención a este tema. Zonas inundables, corrimientos de tierras, etc.
- El edificio debe disponer de las correspondientes instalaciones de detección y sofocación de incendios. En el CPD este no debe ser agresivo con el hardware (debe estar basado en CO2 o espuma, generalmente no en agua).
- La instalación del CPD debe estar preparada (detectores, bombas de achique, falsos suelos, ...) ante posibles inundaciones, bien por averías del edificio (rotura de tuberías), bien por causas atmosféricas.

Entorno - Amenazas externas y Ambientales (II)

14

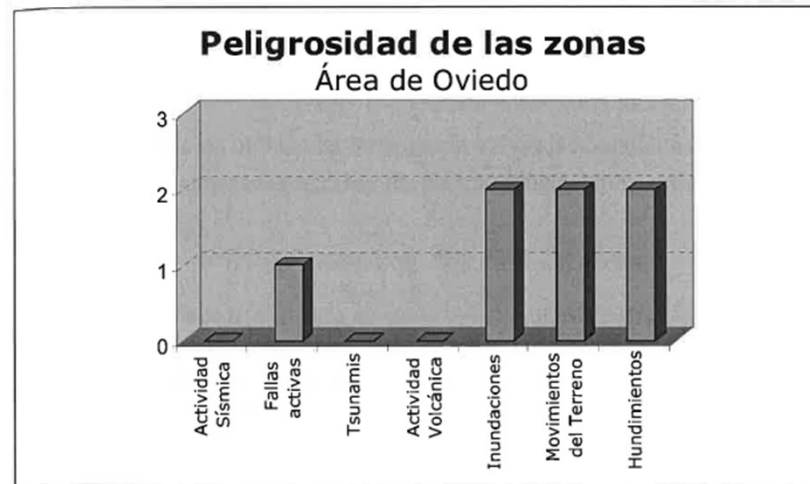


Figura 7 Fuente: Instituto Geológico y Minero de España

En cuanto al impacto de riesgo geológico para el área de Oviedo, zona donde se ubican las instalaciones, y según se muestra en el gráfico adjunto de la página anterior, presenta un riesgo nulo de sufrir desastres por actividad sísmica, Tsunamis y erupciones volcánicas; un riesgo bajo de sufrir desastres por fallas activas; y un riesgo moderado ante desastres por inundaciones, movimientos del terreno o hundimientos.

5.2.2 Desastres Naturales

Garantía de que las instalaciones están protegidas contra desastres naturales: existencia de sistemas de evacuación ante inundaciones; protección contra vendavales, sismos, rayos, etc.; resistencia de techo y estructura; etc.

Aspectos positivos:

Diagnóstico de Seguridad de los Sistemas de Información. PFC cód. DMKPC-0737. EUITIO

Entorno - Suministro de energía (I)¹⁵



- Para que los equipos informáticos puedan trabajar necesitan un suministro de energía estable y sin interrupciones.
- El suministro eléctrico debe estar convenientemente protegido ante sobretensiones.
- La instalación eléctrica debe estar protegida ante posibles ataques, bien desde el interior del edificio (diseño adecuado de la instalación mediante separación de fases, ...) o bien desde el exterior (acometidas eléctricas protegidas).
- El suministro será más seguro cuantos más grados de redundancia integre:
 - En las líneas de la compañía que nos suministre electricidad.
 - Puede ser interesante tener contratada electricidad a varias compañías con sistemas de distribución independientes. Otra forma común de lograr redundancia es instalando un generador (o varios) eléctrico.
 - Dentro del edificio, en los circuitos de alimentación del CPD.

Entorno - Suministro de energía (II)¹⁶

5.2.3 Sistema Eléctrico

Verifica que el suministro de fluido eléctrico mantiene sus características principales: garantía del suministro y conocimiento del tendido; estabilidad de suministro y controles del tendido; existencia de SAI, SAI, grupos electrógenos; diversificación de suministro e iluminación de emergencia; etc.

Aspectos positivos:

- + (I) El suministro eléctrico del edificio de la Facultad de Ciencias se considera fiable a la vista de las estadísticas de pérdidas de suministro proporcionadas por **Hidrocantábrico** al **Vicerrectorado de Infraestructuras**.
- + (I) Se controla la estabilidad y el voltaje de la línea en la Sala de Máquinas y los laboratorios.
- + (I) Todas las zonas de los edificios de la Facultad de Ciencias, Facultad de Geología y Facultad de Magisterio disponen de alumbrado de emergencia, cuyo mantenimiento es responsabilidad del **Vicerrectorado de Infraestructuras** quien lo ha subcontratado a la empresa **Eulen**. El alumbrado es comprobado regularmente, así como la verificación del estado del cableado (incluyendo puntos de iluminación, tomas de energía).
- + (N) Los cables de suministro eléctrico están protegidos por tubos rígidos en las bajantes dentro del edificio, y por canaletas metálicas en el exterior.

Aspectos negativos:

- (I) **RF100**
No se dispone de esquemas eléctricos actualizados.
- (I) **RF101**
Se desconoce si se pasan inspecciones técnicas de los sistemas eléctricos, así como su alcance y periodicidad.

Diagnóstico de Seguridad de los Sistemas de Información. PFC cód. DMKPC-0737. EUITIO

Entorno - Comunicaciones

- El diseño de la red interna del edificio y del CPD debe realizarse de manera que no sea factible caídas generalizadas de la misma.
- Se logrará con un diseño donde haya redundancia tanto de equipos (routers, concentradores, ...) como de cableado.
- Como prevención ante posibles ataques desde dentro del edificio:
 - El cableado y el equipamiento de red no debe estar accesible, sino que debe estar convenientemente oculto y protegido dentro de falsos techos, suelos técnicos, etc.
 - No deben dejarse accesibles bocas de red ni otro tipo de equipamiento sin vigilancia. Un intruso podría conectar ahí un portátil u otro tipo de equipamiento espía.

Entorno - Seguridad en despachos

- Visibilidad desde el exterior
 - Debe vigilarse que el trabajo de los usuarios no sea observable desde el exterior del edificio.
 - Para ello, el monitor y el teclado deben estar orientados de tal manera que un “espía” no pueda ver su contenido ni lo que se teclea.
- Cámaras de seguridad
 - Su instalación puede ser interesante cuando se alberguen datos valiosos.
 - Deben usarse siguiendo una política establecida por la empresa y de acuerdo con la legislación al respecto.

Entorno - Trabajo en áreas seguras

- Además de proteger los sistemas informáticos, todas las medidas que se adopten tienen que tener en cuenta la seguridad del personal que pueda estar trabajando.
- Deben redactarse planes de evacuación ante cualquier circunstancia que pueda ser peligrosa.
- Debe formarse al personal en relación a las medidas de seguridad adoptadas que les incumban directamente.

5.2.6 Fuego (Prevención)

Análisis de las medidas aplicadas para la prevención de fuegos: existencia de vías libres en caso de siniestro; presencia limitada de materiales combustibles; puertas, paredes y falso techo resistente al fuego; impartición de cursillos de formación y simulacros de incendios; prevención eléctrica contra el fuego, diseños resistentes al fuego; etc.

Aspectos positivos:

- + (I) El material de primeros auxilios está guardado en conserjería, en un armario adecuadamente cerrado y señalizado pintado de blanco con una cruz roja. Puede utilizarse en cualquier momento en caso de ser necesario.
- + (I) Cuentan con extintores colocados estratégicamente y con indicadores visibles que facilitan su localización. Los extintores son revisados dentro de los plazos establecidos por la ley, para garantizar su funcionamiento en el momento que sean necesarios.






Diagnóstico de Seguridad de los Sistemas de Información. PFC cód. DMKPC-0737. EUITIO

Entorno - Warchalking

20

- El warchalking es una técnica en comunidades hacker consistente en pintar en la fachada de los edificios símbolos con información sobre redes wifi disponibles en el exterior del mismo.
- Es recomendable inspeccionar la fachada del edificio y sospechar de cualquier marca extraña. Ante la aparición de éstas, pueden desplegarse medidas excepcionales de vigilancia y de actuación.

let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid  bandwidth
CLOSED NODE	ssid 
WEP NODE	ssid access contact  bandwidth
blackbeltjones.com/warchalking	





Seguridad física del equipamiento

Además de las medidas sobre el edificio en general, hay que considerar otras específicas relativas al hardware.

1. Instalación
2. Acceso físico al hardware
3. Plan de evacuación
4. Suministro de energía
5. Tratamiento del calor
6. Disposición del cableado
7. Backups
8. Redundancia
9. Retirada del hardware
10. Seguridad fuera de las instalaciones

Equipamiento físico – Instalación equipos

- Es importante hacer una planificación cuidadosa del espacio disponible y de los dispositivos a instalar.
- Una cuestión vital para el buen funcionamiento del equipo es la calidad de los mismos. Habrá que evaluar la relación coste/calidad a la hora de adquirir equipos en función de los parámetros de la empresa.
- La instalación en armarios o racks es recomendable, dado que pueden ser protegidos por el mismo.
- Hay que reservar espacio en los propios racks para los SAIs, dado que son fundamentales para el buen funcionamiento del sistema.





Equipamiento físico - Acceso físico al hardware

- Independientemente de que el acceso al CPD esté restringido, cada usuario debe tener sólo acceso físico a aquellas máquinas (concentradores, hubs, PCs, ...) a las que está autorizado.
- Deben ser “imposibles” de abrir, para evitar robos o manipulaciones. De nada sirven el resto de medidas si un usuario puede abrir la caja o forzar la cerradura (*lock picking*) de un rack y sustraer algún componente.
- Los dispositivos de grabación deben ser inutilizados si la política de la empresa así lo determina (configuración del SO, modificación hardware, etc), para evitar extracción no autorizada de información.

Equipamiento físico - Plan de evacuación

- Es interesante contar con un plan para el caso de que el hardware tenga que ser evacuado por cualquier contingencia. Dicho plan debe detallar cómo y a dónde se puede trasladar el hardware crítico para el funcionamiento de la empresa en el menor tiempo posible.
- Dicho plan tiene que especificar en qué orden se van a evacuar los distintos dispositivos, en función de la importancia de los datos que contengan y de los procesos que soporten.

Equipamiento físico - Suministro Energía ²⁵

- Todos los elementos hardware deben estar protegidos de sobretensiones y fallos puntuales de suministro mediante SAIs (sistemas de alimentación ininterrumpidos – UPSs).
- La planificación de los SAIs debe ser adecuada (uno grande común/ varios individuales por grupos de equipos)
- La instalación eléctrica debe estar adecuadamente estudiada y preparada con cuadros de protección, limitadores de tensión, etc.



Grado en Ingeniería Informática del Software
Seguridad de Sistemas Informáticos

Equipamiento físico - Tratamiento del calor (I)

- Todos los dispositivos informáticos generan una cantidad de calor que puede ser considerable. Dicho calor tiene que ser “alejado” del dispositivo para evitar daños por sobrecalentamiento o degradación del rendimiento.
- La gestión de la refrigeración debe comenzar por una buena disposición de los equipos (pasillos fríos / pasillos calientes).
- Si el número de equipos lo hace necesario, es preciso instalar sistemas de aire acondicionado. Si no es necesario, hay que asegurar en cualquier caso una correcta ventilación del local.
- Hay que prever la avería de los aparatos de ventilación instalados (en su caso): sistemas redundantes, sistemas alternativos, etc.

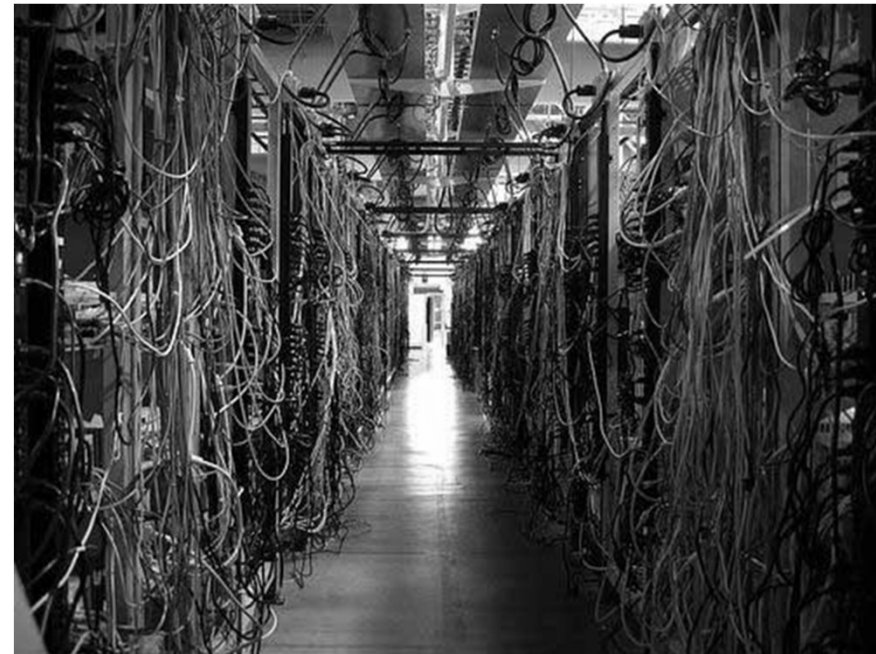
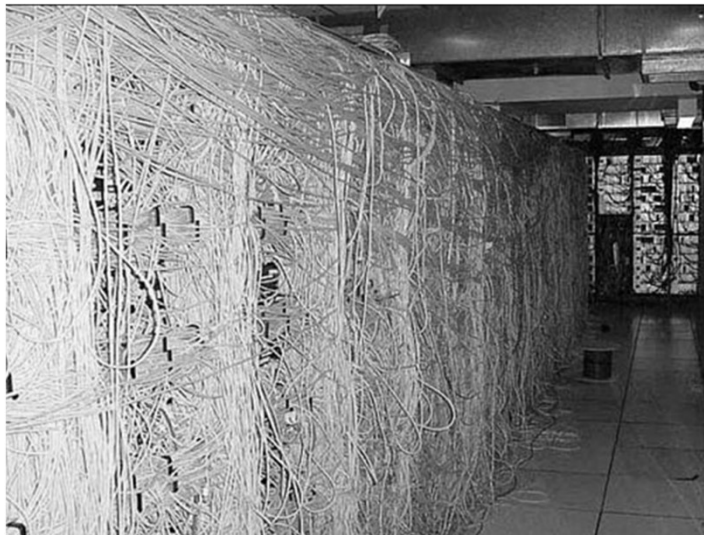
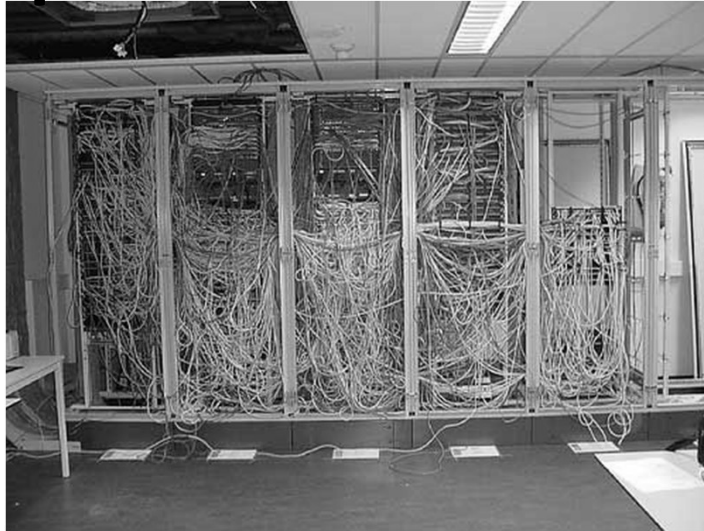
Equipamiento físico - Tratamiento del calor (II)

- La propia instalación en racks puede conllevar la acumulación de calor, con lo que deberá escogerse modelos con ventilación en caso necesario.
- También es preciso contar con sistemas de monitorización de la temperatura, tanto en cada equipo como en los armarios y en distintos puntos de la sala donde estén instalados. Mediante el software adecuado (ej. *Nagios*) pueden lanzarse alarmas en caso de incidencias.
- Los ordenadores actualmente permiten ser configurados para que avisen en caso de sobrecalentamiento, que varíen la velocidad de sus ventiladores, etc.

Equipamiento físico - Disposición del cableado

- En la instalación pueden convivir, entre otros, cableado eléctrico, cableado de red coaxial, cableado de red de “par trenzado”, cableado óptico y cableado telefónico.
- En general, todo el cableado de datos basado en impulsos eléctricos puede verse perturbado por los campos electromagnéticos generados por las conducciones eléctricas.
- La instalación debe hacerse de tal forma que tales interferencias sean mínimas (“blindando” los cables eléctricos y/o de datos, conduciéndolos por vías distintas, etc).

Equipamiento físico - Disposición del cableado



Equipamiento físico - Backups

- Debe tenerse claramente establecida una política de realización de backups, que determine cuándo se hacen copias, de qué se hacen copias y sobre qué dispositivo.
- Debe contemplarse la seguridad de las copias realizadas. En datos críticos pueden realizarse múltiples copias y almacenarlas:
 - a) En armarios ignífugos.
 - b) En distintas estancias del edificio.
 - c) En edificios distintos.
 - d) Externalizando su almacenamiento /realización.

5.3.2 Copias de Respaldo y Procedimientos de Recuperación

Aspectos positivos:

- + (I) Los becarios hacen Copia de Respaldo del servidor web de **EUITIO**.
- + (N) Cada equipo del laboratorio tiene una imagen, almacenada en CD-ROM, que permite recuperar la configuración del sistema en poco tiempo.

Aspectos negativos:

- (I) **RL100**
No existe una política para la realización de Copias de Respaldo y los procedimientos de Recuperación.
- (I) **RL101**
No existe un lugar centralizado para custodiar las Copias de Respaldo realizadas.
- (I) **RL102**
No existen ordenadores de respaldo para el caso de caída de los equipos principales.

Diagnóstico de Seguridad de los Sistemas de Información. PFC cód. DMKPC-0737. EUITIO

Equipamiento físico - Redundancia ³¹



- La seguridad ante averías (fortuitas o provocadas) de los equipos suele lograrse por medio de la redundancia de los equipos.
- Esta redundancia puede darse a distintos niveles:
 - A nivel de máquinas (clústers, nubes, ...)
 - Redundancia de componentes (procesador, memoria, fuentes de alimentación, ...) Es interesante, en cualquier caso, que además de redundantes tengan características de *hot-swap*.
 - A nivel de datos, replicando el contenido de los sistemas de almacenamiento en otros (preferiblemente en otra ubicación).
- Como ya se ha comentado previamente, también los sistemas eléctricos, de red, de refrigeración, ..., deberían ser redundantes.

Equipamiento físico - Retirada de hardware

- Puede encontrarse mucha información útil para un ataque hurgando en los deshechos de una organización (*Dumpster diving*).

<http://searchsecurity.techtarget.com/definition/dumpster-diving>

- Debe establecerse una política adecuada de tratamiento del mismo (destrucción, gestión por una empresa externa, etc).

(Ya que estamos...

http://tecnologia.elpais.com/tecnologia/2015/06/12/actualidad/1434096507_068330.html)



Equipamiento físico- Seguridad fuera de las instalaciones ³³



- Especial atención merecen los dispositivos portátiles ya que por sus propias características, son susceptibles de ser robados.
- Su salida de la empresa debe ser justificada, y debe estar en todo momento controlada.
- No deberían contener información valiosa: es mejor que sirvan sólo como terminales remotas. Si es necesario almacenar localmente información, debe hacerse de manera encriptada.
- Todo usuario que los utilice debe estar concienciado de las políticas de seguridad de la empresa y de las condiciones de uso de los mismos.
- Todos los equipos al volver a la empresa deberían ser comprobados para localizar virus, troyanos, software instalado, ...

**Más de 12.000 portátiles perdidos
cada día**

En Aeropuertos de
EEUU



- Las políticas de seguridad respecto al personal tratan de:
 - Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización.
 - Prevenir las exposiciones a riesgos y a robos de la información y de recursos de tratamiento de información: guardar los recursos en cajones con llave y/o en archivadores.
- Como parte de esta política de seguridad debería contemplarse:
 - No dejar funciones y equipos de soporte desatendidos, por ejemplo si se está imprimiendo información confidencial de la empresa.
 - Utilizar en todos los puestos de trabajo protector de pantalla con contraseña.
- Deberían implantarse controles de seguridad que abarquen el ciclo de vida de los trabajadores, desde su selección hasta el momento en que dejen la organización.