VALORAR EL AMBIENTE FÍSICO DE LA RED.

1. Control de condiciones ambientales.
2. Ergonomía del ambiente físico.
3. Sistema de cableado estructurado.
4. Instalación eléctrica.
5. Normas de seguridad e higiene.

1. Control de condiciones ambientales.

Las computadoras son sensibles al ambiente físico y por lo regular necesitan condiciones especiales, como:

• **Aire acondicionado** -los equipos de cómputo normalmente requieren temperaturas templadas.

• **Minimización de polvo** -el polvo es muy dañino para la operación de los equipos de cómputo-, la limpieza regular para eliminar el polvo y la mugre es esencial, en algunos casos se requiere equipo de filtración de aire especial para remover todo el polvo.

• **Control de humedad** -la humedad también puede ser dañina para los equipos de cómputo-, los ambientes muy secos o muy fríos también pueden provocar problemas, particularmente la oxidación de artículos metálicos.

• **Prevención de incendios** -por su naturaleza eléctrica, los equipos de cómputo son susceptibles al fuego, es necesario contar con alarmas de detección de incendios, extinguidores y planes operativos contra incendios.

2. Ergonomía del ambiente físico.

La Ergonomía, es una ciencia que busca que el hombre y el entorno creado por sí mismo trabajen en completa armonía. Dejar de considerar los principios de la Ergonomía llevará a diversos efectos negativos que - en general - se expresan en lesiones, enfermedad profesional, o deterioros de productividad y eficiencia.

- **Mobiliario ergonómico** -El personal que utilice equipo de cómputo necesita mesas, sillas y accesorios ergonómicos para minimizar la incidencia de lesiones en el sitio de trabajo.

- Determine la altura de la superficie de trabajo a través de la altura de los codos.
- Ajuste la altura de la superficie de trabajo con base en la tarea que se realiza.
- Proporcione una silla cómoda al operador.
- Proporcione ajustabilidad en el asiento.
- Promueva la fexibilidad postural.
- Coloque todas las herramientas y materiales dentro del área de trabajo normal.

- **iluminación.**

El sentido común nos dice que la calidad del trabajo disminuye cuando no hay luz suficiente. Por otra parte, se sabe que si una iluminación defectuosa se prolonga largo tiempo, el sujeto puede sufrir trastornos visuales.

- **Color.**

Se afirma que el color eleva la producción, aminora accidentes y errores, mejora la moral. Las paredes pintadas de colores claros comunican la sensación de mayor amplitud y apertura.

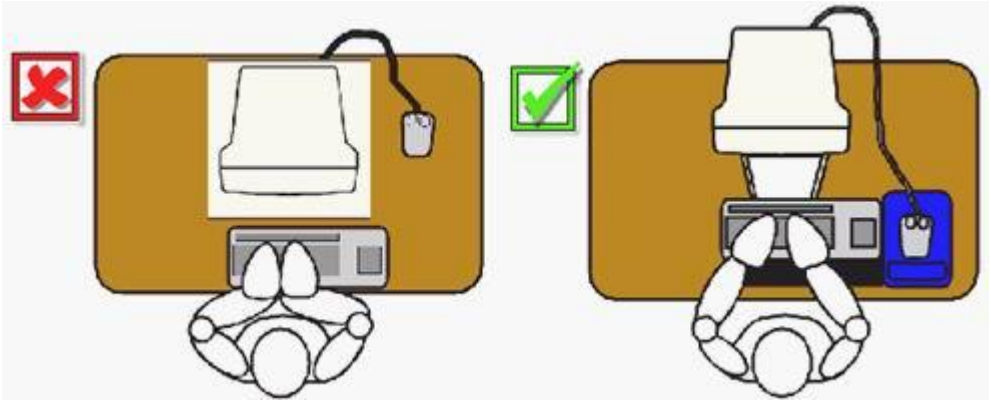
- **Ruido.**

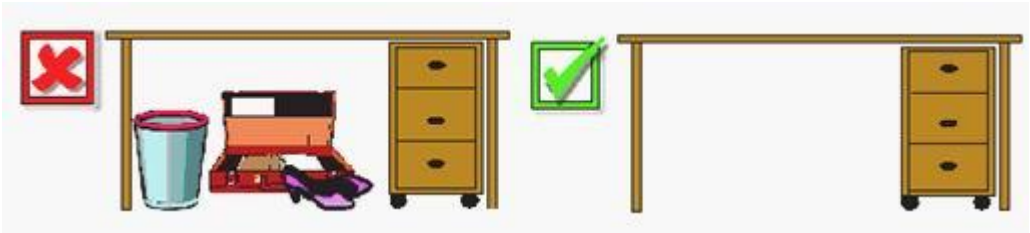
El ruido se considera un sonido o barullo indeseable. Se sabe que ciertas intensidades pueden dañar el oído. Así, si un trabajador diariamente oye sonidos de cierto nivel de decibeles durante largo tiempo, sin duda terminará por sufrir pérdida de la audición.

- **Música.**

Al parecer carece de confirmación la hipótesis de que con música se eleva la productividad en todo tipo de trabajo. El efecto de ella depende de la índole de las labores. Según datos de investigación, con la música se incrementa la productividad en tareas bastante sencillas, repetidas y que no requieran unidades de corta duración, en consecuencia, posiblemente la música se convierte en el foco de atención y hace que la jornada transcurra en forma más rápida y grata.

Las cosas cambian cuando se trata de una labor compleja que exija mucho esfuerzo. No está demostrado que la música eleve la producción de los trabajos difíciles porque se requiere de plena concentración.





3. SISTEMA DE CABLEADO ESTRUCTURADO

El cableado estructurado es la técnica que permite cambiar, identificar y mover periféricos o equipos de una red con flexibilidad y sencillez. Una solución de cableado estructurado debe tener dos características: modularidad, que sirve para construir arquitecturas de red de mayor tamaño sin incrementar la complejidad del sistema, y flexibilidad, que permite el crecimiento no traumático de la red.

Elementos del cableado estructurado

Partiendo del subsistema de más bajo nivel jerárquico, se presenta la siguiente organización:

- Localización de cada puesto de trabajo. A cada puesto deben poder llegar todos los posibles medios de transmisión de la señal que requiera cada equipamiento: UTP, STP, fibra óptica, cables para el uso de transceptores, etcétera.

- Subsistema horizontal o de planta. Es recomendable la instalación de una canaleta o un subsuelo por el que llevar los sistemas de cableado a cada puesto. Las exigencias de ancho de banda pueden requerir el uso de dispositivos especiales para conmutar paquetes de red, o concentrar y repartir el cableado en estrella. En este nivel se pueden utilizar todos los tipos de cableados mencionados: coaxial, UTP, STP, fibra, etc., aunque alguno de ellos, como el coaxial, presentan problemas por su facilidad de ruptura o su fragilidad, especialmente en los puntos de inserción de [t], con la consiguiente caída de toda la red. Sólo si el sistema se compone de un número reducido de puestos, el cable coaxial puede compensar por su facilidad de instalación. Además, no requiere ningún dispositivo activo o pasivo para que la red comience a funcionar. Subsistema distribuidor o administrador. Se pueden incluir aquí los racks, los distribuidores de red con sus latiguillos, etcétera.

Subsistema vertical o backbone. Este subsistema está encargado de comunicar todos los subsistemas horizontales por lo que requiere de medios de transmisión de señal con un ancho de banda elevado y de elevada protección. Para confeccionar un backbone se puede utilizar: cable coaxial fino o grueso (10 Mbps), fibra óptica u otro tipo de medios de transmisión de alta velocidad. También se pueden utilizar cables de pares, pero siempre en configuración de estrella utilizando concentradores especiales para ello. Los backbones más modernos se construyen con tecnología de redes FDDI o Gigabit Ethernet. Este tipo de comunicaciones es ideal para su uso en instalaciones que requieran de aplicaciones multimedia.

- Subsistema de campus. Extiende la red de área local al entorno de varios edificios, por tanto, en cuanto a su extensión se parece a una red MAN, pero mantiene toda la funcionalidad de una red de área local. El medio de transmisión utilizado con mayor frecuencia es la fibra óptica con topología de doble anillo.

- Cuartos de entrada de servicios, telecomunicaciones y equipos. Son los lugares apropiados para recoger las entradas de los servicios externos a la organización (líneas telefónicas, accesos a Internet, recepción de TV por cable o satélite, etc.), la instalación de la maquinaria de comunicaciones y para los equipamientos informáticos centralizados. En algunas organizaciones existen los tres tipos de espacios; en otras, el cuarto de equipos incluye al de telecomunicaciones y el de entrada de servicios es sustituido por un armario receptor. Aunque no es estrictamente indispensable, se recomienda un cuarto de comunicaciones por cada planta.

Figura 3.36. Cableado estructurado desde el cuarto de comunicaciones hasta el usuario final.

La especificación de cableado estructurado exige que los cables no superen los 90 m de longitud, teniendo en cuenta que se pueden añadir 10 m más para los latiguillos inicial y final, de modo que el canal de principio a fin no supere los 100 m, que es la distancia permitida por los cables UTP de categoría 5e. También se especifican, por ejemplo, las distancias que hay que dejar alrededor de los armarios para que se pueda trabajar cómodamente en ellos. Los estándares más comunes sobre cableado estructurado son en ANSI/TIA/EIA-568 y ANSI/TIA/EIA-569. Los armarios y distribuidores deben cumplir el estándar ANSI/EIA-310.

Etiquetado de los cables

La norma EIA/TIA-606 especifica que cada terminación de hardware debe tener alguna etiqueta que lo identifique de manera exclusiva. Un cable tiene dos terminadores, por tanto, cada uno de estos extremos recibirá un nombre.

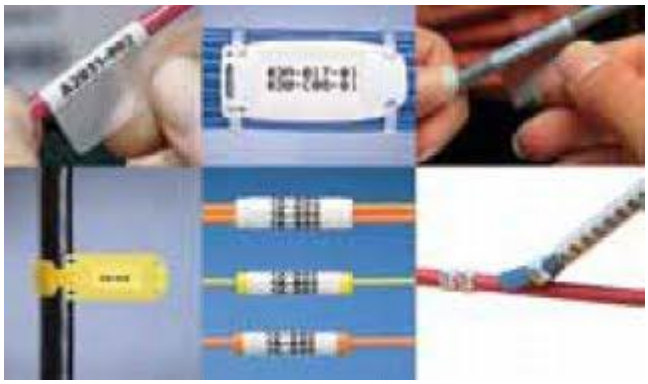
No es recomendable la utilización de un sistema de etiquetado con relación a un momento concreto, es mejor, utilizar nomenclaturas neutras. Por ejemplo, si etiquetamos un PC como [pc-dirección], y luego cambia el lugar del edificio en donde se ubica la Dirección, habría que cambiar también el etiquetado, sin embargo, se trata de que el etiquetado sea fijo.

Se recomienda la utilización de etiquetas que incluyan un identificador de sala y un identificador de conector, así se sabe todo sobre el cable: dónde empieza y dónde acaba. Por ejemplo, se podría etiquetar un cable con el siguiente identificador:

03RS02-05RS24

Este cable indicaría que está tendido desde la roseta (RS) número 02 de la sala 03 hasta la roseta 24 de la sala 05. Las rosetas en las salas 03 y 05 irían etiquetadas con 03RS02 y 05RS24 respectivamente.

Algunos modelos de etiquetas para cables.



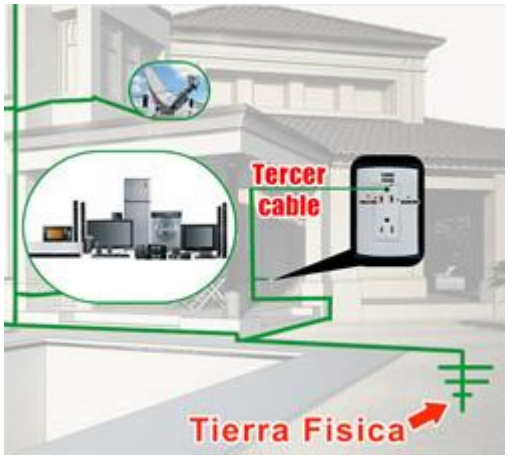
El cableado estructurado

Los cambios que se deben realizar en las instalaciones de red, especialmente en su cableado son frecuentes debido a la evolución de los equipos y a las necesidades de los usuarios de la red. Esto nos lleva a tener en cuenta otro factor importante: la flexibilidad. Un sistema de cableado bien diseñado debe tener al menos estas dos cualidades: seguridad y flexibilidad. A estos parámetros se le pueden añadir otros, menos exigentes desde el punto de vista del diseño de la red, como son el coste económico, la facilidad de instalación, etcétera.

4. INSTALACIÓN ELÉCTRICA

Es muy importante que la instalación eléctrica esté muy bien hecha. De no ser así, se corren riesgos importantes, incluso de electrocución. Los problemas eléctricos suelen generar problemas intermitentes muy difíciles de diagnosticar y provocan deterioros importantes en los dispositivos de red. Todos los dispositivos de red deben estar conectados con enchufes a tierra. Las carcasas de estos dispositivos, los armarios, las canaletas mecánicas, etc., también deben ser conectadas a tierra.

Toda la instalación debe estar a su vez conectada a la tierra del edificio en el que habrá que cuidar que el número de picas que posee es suficiente para lograr una tierra aceptable. Otro problema importante que hay que resolver viene originado por los cortes de corriente o las subidas y bajadas de tensión. Para ello se pueden utilizar sistemas de alimentación ininterrumpida. Normalmente, los **Sistemas de alimentación ininterrumpida (SAI)** corrigen todas las deficiencias de la corriente eléctrica, es decir, actúan de estabilizadores, garantizan el fluido frente a cortes de corriente, proporcionan el flujo eléctrico adecuado, etcétera.



Diversos modelos de SAI.

El SAI contiene en su interior unos acumuladores que se cargan en el régimen normal de funcionamiento. En caso de corte de corriente, los acumuladores producen la energía eléctrica que permite guardar los datos que tuvieran abiertos las aplicaciones de los usuarios y cerrar ordenadamente los sistemas operativos. Si además no se quiere parar, hay que instalar grupos electrógenos u otros generadores de corriente conectados a nuestra red eléctrica.

Básicamente hay dos tipos de SAI:
- SAI de modo directo. La corriente eléctrica alimenta al SAI y éste suministra energía constantemente al ordenador. Estos dispositivos realizan también la función de estabilización de corriente.
- SAI de modo reserva. La corriente se suministra al ordenador directamente. El SAI sólo actúa en caso de corte de corriente.

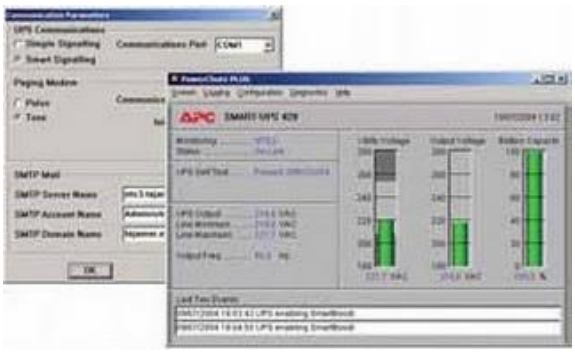


Figura 3.30. Parámetros configurables en una estación para el gobierno de un SAI.

Los servidores pueden comunicarse con un SAI a través de alguno de sus puertos de comunicaciones, de modo que el SAI informa al servidor de las incidencias que observa en la corriente eléctrica. En la Figura 3.30 se pueden observar algunos de los parámetros que se pueden configurar en un ordenador para el gobierno del SAI. Windows, por ejemplo, lleva ya preconfigurados una lista de SAI de los principales fabricantes con objeto de facilitar lo más posible la utilización de estos útiles dispositivos.

5. Normas de seguridad e higiene.

Seguridad Física

Garantizar la seguridad física de la tecnología es una de las vías fundamentales para minimizar los riesgos en su uso.

Las medidas de seguridad física pueden ser divididas en dos grandes categorías: contra factores ambientales como el fuego, la humedad, las inundaciones, el calor o el frío y los fallos en el suministro de energía; y **contra interferencias humanas** sean deliberadas o accidentales.

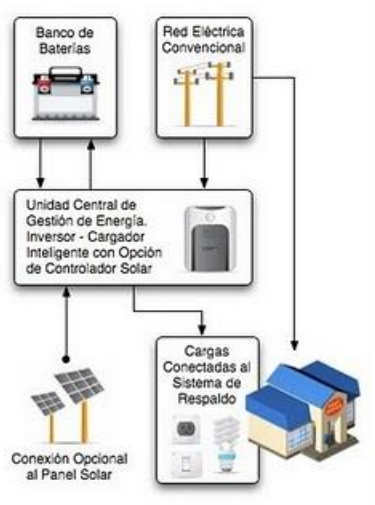
Contra factores ambientales

Cuando la tecnología es alimentada por electricidad (y la mayoría lo es), la seguridad de la fuente de energía es crucial.

Una fuente común de respaldo de energía es el denominado **Suministro de Energía Ininterrumpible (UPS por sus siglas en inglés).** Suele conectarse un UPS entre la principal fuente de energía y el componente tecnológico, como un equipo de cómputo. Si la principal fuente de suministro falla, la batería incluida en el UPS entra en operación inmediatamente y se hace cargo del suministro de energía.

Algunos sistemas UPS son lo suficientemente poderosos para mantener el sistema en operación por un periodo prolongado, por lo que es posible que los usuarios ni siquiera se percaten que la principal fuente de suministro ha fallado y pueden seguir trabajando. Sin embargo, como esta clase de sistemas UPS requieren de potentes baterías para operar, suelen ser muy costosos. Otro tipo de sistemas UPS menos costoso no pueden servir como sistemas de reemplazo durante mucho tiempo.

Las descargas pueden ser peligrosas para los equipos de cómputo y pueden quemar fusibles o componentes del equipo. Un sistema UPS intercepta una sobrecarga y evita que llegue a un equipo sensible.



Otro aspecto importante de la seguridad física es asegurar que el equipo tecnológico, especialmente el de cómputo, esté debidamente resguardado. Idealmente, el equipo de cómputo debe ser almacenado en edificios sellados con control de clima, para que la temperatura y la humedad se mantengan a un nivel óptimo constante y se eliminen contaminantes como la suciedad, el polvo y el humo. Es usual que los sistemas convencionales de aire acondicionado que

se utilizan para controlar la temperatura en los edificios se empleen para estos efectos.
El equipo de comunicación es otro tipo de tecnología que requiere seguridad física especial. En particular los cables de conexión de las redes de cómputo requieren gran seguridad. Entre las formas de proteger los cables contra la amenaza de roedores o humanos puede ser colocarlos dentro de ductos, tras paredes, bajo piso o bajo techo, instalar pisos falsos para permitir que los cables circulen sin problema, enterrarlos o montarlos sobre poleas. Cuando los cables estén en riesgo, se pueden considerar alternativas como las de enlace a través de microondas.

Contra factores humanos
El aislamiento físico, como colocar componentes clave o los servidores de las redes en salones especiales, puede ayudar a reducir la posibilidad de intervención humana. De igual forma, colocar los cables de las redes dentro de las paredes o bajo suelos y techos torna difícil acceder a ellos.La medida física más efectiva que se puede tomar para prevenir la intervención humana es la de ubicar la tecnología dentro de sitios seguros bajo llave.

La tecnología moderna ofrece un amplio catálogo de dispositivos sofisticados que pueden restringir la entrada a edificios o salones solo al personal autorizado.

Entre ellos:
• Candados y cerrojos convencionales.
• Cerrojos operados por códigos de acceso (mecánico o automatizado).
• Cerrojos operados por tarjetas con bandas magnéticas.
• Cerrojos que reconocen rasgos físicos, como las huellas dactilares, de la mano o la retina.
• Cerrojos que requieren una combinación de dos o más de estos dispositivos.

NORMAS DE SEGURIDAD E HIGIENE

Se requiere tomar en cuenta las medidas de prevención y seguridad siguientes:

No entrar con mochilas.
No consumir bebidas o alimentos en el área de trabajo.
No sentarse en las mesas.
Acomodar las sillas al terminar.
No fumar.
Guardar silencio.
Cuidar el equipo.
Si hubiese una dificultad técnica en el funcionamiento de algún equipo, deberá de ser reportado con el responsable del área.
No tirar basura.
No desconectar equipos, conexiones de corriente o de red.
No instalar ningún tipo de software al equipo.
Desinfectar cualquier medio de almacenamiento externo antes de abrirlo con el uso del antivirus.

La forma final de seguridad contra la intervención humana es la de dificultar o hacer imposible que una persona no autorizada pueda acceder o modificar los datos contenidos en un sistema de cómputo. Esto se puede lograr a través del uso de contraseñas y del encriptamiento.