**Seguridad física**

Cuando hablamos de seguridad física nos referimos a todos aquellos mecanismos generalmente de prevención y detección destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina. Dependiendo del entorno y los sistemas a proteger esta seguridad será más o menos importante y restrictiva, aunque siempre deberemos tenerla en cuenta. A continuación mencionaremos algunos de los problemas de seguridad física con los que nos podemos enfrentar y las medidas que podemos tomar para evitarlos o al menos minimizar su impacto.

**Protección del hardware**

El hardware es frecuentemente el elemento más caro de todo sistema informático y por tanto las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización.

Problemas a los que nos enfrentamos:

Acceso físico

Desastres naturales

Alteraciones del entorno

Acceso físico

Si alguien que desee atacar un sistema tiene acceso físico al mismo todo el resto de medidas de seguridad implantadas se convierten en inútiles. De hecho, muchos ataques son entonces triviales, como por ejemplo los de denegación de servicio; si apagamos una máquina que proporciona un servicio es evidente que nadie podrá utilizarlo. Otros ataques se simplifican enormemente, p. ej. si deseamos obtener datos podemos copiar los ficheros o robar directamente los discos que los contienen. Incluso dependiendo el grado de vulnerabilidad del sistema es posible tomar el control total del mismo, por ejemplo reiniciándolo con un disco de recuperación que nos permita cambiar las claves de los usuarios. Este último tipo de ataque es un ejemplo claro de que la seguridad de todos los equipos es importante, generalmente si se controla el PC de un usuario autorizado de la red es mucho más sencillo atacar otros equipos de la misma. Para evitar todo este tipo de problemas deberemos implantar mecanismos de prevención (control de acceso a los recursos) y de detección (si un mecanismo de prevención falla o no existe debemos al menos detectar los accesos no autorizados cuanto antes). En muchos casos es suficiente con controlar el acceso a las salas y cerrar siempre con llave los despachos o salas donde hay equipos informáticos y no tener cableadas las tomas de red que estén accesibles. Para la detección de accesos se emplean medios técnicos, como cámaras de vigilancia de circuito cerrado o alarmas, aunque en muchos entornos es suficiente con qué las personas que utilizan los sistemas se conozcan entre si y sepan quien tiene y no tiene acceso a las distintas salas y equipos, de modo que les resulte sencillo detectar a personas desconocidas o a personas conocidas que se encuentran en sitios no adecuados.

**Desastres naturales**

Además de los posibles problemas causados por ataques realizados por personas, es importante tener en cuenta que también los desastres naturales pueden tener muy graves consecuencias, sobre todo si no los contemplamos en nuestra política de seguridad y su implantación.

Algunos desastres naturales a tener en cuenta: Terremotos y vibraciones Tormentas eléctrica Inundaciones y humedad Incendios y humos

Los terremotos son el desastre natural menos probable en la mayoría de organismos ubicados en España, por lo que no se harán grandes inversiones en prevenirlos, aunque hay varias cosas que se pueden hacer sin un desembolso elevado y que son útiles para prevenir problemas causados por pequeñas vibraciones: No situar equipos en sitios altos para evitar caídas,

No colocar elementos móviles sobre los equipos para evitar que caigan sobre ellos, separar los equipos de las ventanas para evitar que caigan por ellas o qué objetos lanzados desde el exterior los dañen. Utilizar fijaciones para elementos críticos. Colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones,

Otro desastre natural importante son las tormentas con aparato eléctrico, especialmente frecuentes en verano, que generan subidas súbitas de tensión muy superiores a las que pueda generar un problema en la red eléctrica. A parte de la protección mediante el uso de pararrayos, la única solución a este tipo de problemas es desconectar los equipos antes de una tormenta (qué por fortuna suelen ser fácilmente predecibles).

En entornos normales es recomendable que haya un cierto grado de humedad, ya que en si el ambiente es extremadamente seco hay mucha electricidad estática. No obstante, tampoco interesa tener un nivel de humedad demasiado elevado, ya que puede producirse condensación en los circuitos integrados que den origen a un cortocircuito. En general no es necesario emplear ningún tipo de aparato para controlar la humedad, pero no está de más disponer de alarmas que nos avisen cuando haya niveles anómalos.

Otro tema distinto son las inundaciones, ya que casi cualquier medio (máquinas, cintas, routers) que entre en contacto con el agua queda automáticamente inutilizado, bien por el propio líquido o bien por los cortocircuitos que genera en los sistemas electrónicos. Contra ellas podemos instalar sistemas de detección que apaguen los sistemas si se detecta agua y corten la corriente en cuanto estén apagados. Hay que indicar que los equipos deben estar por encima del sistema de detección de agua, sino cuando se intente parar ya estará mojado.

Por último mencionaremos el fuego y los humos, que en general provendrán del incendio de equipos por sobrecarga eléctrica. Contra ellos emplearemos sistemas de extinción, que aunque pueden dañar los equipos que apaguemos (aunque actualmente son más o menos inocuos), nos evitarán males mayores. Además del fuego, también el humo es perjudicial para los equipos (incluso el del tabaco), al ser un abrasivo que ataca a todos los componentes, por lo que es recomendable mantenerlo lo más alejado posible de los equipos.

**Alteraciones del entorno**

En nuestro entorno de trabajo hay factores que pueden sufrir variaciones que afecten a nuestros sistemas que tendremos que conocer e intentar controlar. Deberemos contemplar problemas que pueden afectar el régimen de funcionamiento habitual de las máquinas como la alimentación eléctrica, el ruido eléctrico producido por los equipos o los cambios bruscos de temperatura.

**Electricidad**

Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta nuestros equipos; cortocircuitos, picos de tensión, cortes de flujo Para corregir los problemas con las subidas de tensión podremos instalar tomas de tierra o filtros reguladores de tensión.

Para los cortes podemos emplear Sistemas de Alimentación Ininterrumpida (SAI), que además de proteger ante cortes mantienen el flujo de corriente constante, evitando las subidas y bajadas de tensión. Estos equipos disponen de baterías que permiten mantener varios minutos los aparatos conectados a ellos, permitiendo que los sistemas se apaguen de forma ordenada (generalmente disponen de algún mecanismo para comunicarse con los servidores y avisarlos de que ha caído la línea o de que se ha restaurado después de una caída).

Por último indicar que además de los problemas del sistema eléctrico también debemos preocuparnos de la corriente estática, que puede dañar los equipos. Para evitar problemas se pueden emplear espráis antiestáticos o ionizadores y tener cuidado de no tocar componentes metálicos, evitar que el ambiente esté excesivamente seco, etc.

**Ruido eléctrico**

El ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también puede serlo por otros ordenadores o por multitud de aparatos, y se transmite a través del espacio o de líneas eléctricas cercanas a nuestra instalación. Para prevenir los problemas que puede causar el ruido eléctrico lo más barato es intentar no situar el hardware cerca de los elementos que pueden causar el ruido. En caso de que fuese necesario hacerlo siempre podemos instalar filtros o apantallar las cajas de los equipos.

**Temperaturas extremas**

No hace falta ser un genio para comprender que las temperaturas extremas, ya sea un calor excesivo o un frio intenso, perjudican gravemente a todos los equipos. En general es recomendable que los equipos operen entre 10 y 32 grados Celsius. Para controlar la temperatura emplearemos aparatos de aire acondicionado.

**Protección de los datos**

Además proteger el hardware nuestra política de seguridad debe incluir medidas de protección de los datos, ya que en realidad la mayoría de ataques tienen como objetivo la obtención de información, no la destrucción del medio físico que la contiene.

En los puntos siguientes mencionaremos los problemas de seguridad que afectan a la transmisión y almacenamiento de datos, proponiendo medidas para reducir el riesgo.

**Copias de seguridad**

Es evidente que es necesario establecer una política adecuada de copias de seguridad en cualquier organización; al igual que sucede con el resto de equipos y sistemas, los medios donde residen estas copias tendrán que estar protegidos físicamente; de hecho quizás deberíamos de emplear medidas más fuertes, ya que en realidad es fácil que en una sola cinta haya copias de la información contenida en varios servidores.

Lo primero que debemos pensar es dónde se almacenan los dispositivos donde se realizan las copias. Un error muy habitual es almacenarlos en lugares muy cercanos a la sala de operaciones, cuando no en la misma sala; esto, que en principio puede parecer correcto (y cómodo si necesitamos restaurar unos archivos) puede convertirse en un problema serio si se produce cualquier tipo de desastre (como p. ej. un incendio). Hay que pensar que en general el hardware se puede volver a comprar, pero una pérdida de información puede ser irreemplazable.

Así pues, lo más recomendable es guardar las copias en una zona alejada de la sala de operaciones; lo que se suele recomendar es disponer de varios niveles de copia, una que se almacena en una caja de seguridad en un lugar alejado y que se renueva con una periodicidad alta y otras de uso frecuente que se almacenan en lugares más próximos (aunque a poder ser lejos de la sala donde se encuentran los equipos copiados).

Para proteger más aun la información copiada se pueden emplear mecanismos de cifrado, de modo que la copia que guardamos no sirva de nada si no disponemos de la clave para recuperar los datos almacenados.

**Soportes no electrónicos**

Otro elemento importante en la protección de la información son los elementos no electrónicos que se emplean para transmitirla, fundamentalmente el papel. Es importante que en las organizaciones que se maneje información confidencial se controlen los sistemas que permiten exportarla tanto en formato electrónico como en no electrónico (impresoras, plotters, faxes, teletipos).

Cualquier dispositivo por el que pueda salir información de nuestro sistema ha de estar situado en un lugar de acceso restringido; también es conveniente que sea de acceso restringido el lugar donde los usuarios recogen los documentos que lanzan a estos dispositivos.

Además de esto es recomendable disponer de trituradoras de papel para destruir todos los papeles o documentos que se quieran destruir, ya que evitaremos que un posible atacante pueda obtener información rebuscando en nuestra basura.