Seguridad física

En la década de los 40, cuando los equipos de cómputo eran enormes, generaban grandes cantidades de calor y las velocidades de procesamiento eran muy limitadas, tenían que ubicarse en espacios lo suficientemente grandes para albergarlos, ser operados por personal altamente especializado (generalmente científicos) y debían mantener la temperatura baja para evitar sobrecalentamientos y eventuales daños en sus componentes; sin embargo a pesar de lo anterior, los controles de temperatura, humedad, seguridad y acceso eran muy rudimentarios y limitados.

En la actualidad, las otrora llamadas salas de procesamiento de datos, son espacios (llamados *site*s o Network Operation Center, IT Room, etc.) donde se albergan servidores web, de bases de datos, correo electrónico o servidores de aplicaciones, se toman muy en serio todos los aspectos relacionados con la seguridad física, permitiendo minimizar los efectos relacionados con fenómenos perturbadores como incendios, sismos, inundaciones, contaminación, hacking, entre otros, que amenacen su operación diaria. Algunos elementos que han de tomarse en cuenta son:

- **Acceso al *site***. Debe realizarlo únicamente personal autorizado y especializado. Normalmente el acceso se controla mediante cámaras de vigilancia, lectores de tarjeta o dispositivos biométricos (escaneo de mano, huella dactilar, retina, etc.). En ocasiones se combinan estos elementos fortaleciendo el control de acceso.
- **Espacio climatizado**. Por lo general, todo equipo electrónico genera calor; de hecho, las computadoras poseen uno o más ventiladores que permiten expulsar el aire caliente a través de sus rejillas de ventilación; sin embargo, cuando hay decenas o cientos de computadoras colocadas en un mismo espacio físico, el aumento desmesurado de calor podría dañar sus componentes electrónicos. Por ello, en los *site*s deben existir sistemas de enfriamiento de precisión que regulen la temperatura, manteniéndola en los 21 °C (± 1 °C). También es importante mantener la humedad relativa de 45% (± 2%) y aire filtrado dentro de la sala cercano al 90%, evitando la presencia de polvo que provoca sobrecalentamiento y cargas estáticas dañinas. Todos ellos son factores que garantizarán en buena medida el correcto funcionamiento físico de los equipos.
- **Sistemas de alarma**. Un centro de cómputo debe tener sistemas de alarma que detecten aumentos repentinos de temperatura, incendio, humo, sismo, movimiento o inundación, así como sensores ubicados estratégicamente, que activen estas alarmas.
- **Sprinkers**. Son rociadores de agua o gas inerte, generalmente ubicados en el techo del *site*. Cuando hay presencia de humo o calor, un sensor activa el sistema y automáticamente se encienden, rociando generalmente gas (por tratarse de dispositivos electrónicos no se usa agua) uniformemente por toda la sala.
- **Instalación eléctrica**. Todo *site* debe tener una instalación capaz de soportar la carga consumida por los equipos de cómputo. Calibre de conductores adecuados, centros de carga debidamente balanceados, líneas polarizadas y tierra física apropiadamente instalada. Adicionalmente, debe contar con sistemas de respaldo como No-breaks cuyo tiempo de operación sea el suficiente, al menos para realizar un apagado (shutdown) normal de los equipos. En *site*s donde la operación debe ser continua, es necesario tener bancos de baterías y generadores a diésel que garanticen indefinidamente el suministro de energía.
- **Plan de contingencias**. Este documento es fundamental para toda área de cómputo que presuma de cumplir los estándares mínimos de seguridad informática pues contiene aquellas acciones que deben llevarse a cabo antes, durante y después de la ocurrencia de un siniestro, estando encaminadas a la protección del hardware y software, garantizando la integridad del personal y la operación de al menos los procesos informáticos críticos o prioritarios de la empresa.

Así pues, la seguridad física es un elemento poco conocido por los usuarios pero muy necesario para garantizar la operación y el servicio informáticos de una organización.

REFERENCIAS

- Guil, F. (2003). “Computer Rooms – Meet the physical security measures”. GSEC – Assignment 1 version 1.0. Global Information Assurance Certification. Tomado de: https://www.giac.org/paper/gsec/2892/computer-rooms-meet-physical-security-measures/104866
- Kent, J. (2012). “Ten Ways to Improve the Security of a New Computer”. United States Computer Emergency Readiness Team. Tomado de: https://www.us-cert.gov/sites/default/files/publications/TenWaystoImproveNewComputerSecurity.pdf
- Nuno, P. (2006). “Climatización en el centros de procesamiento de datos”. Enfoques. Tomado de https://www.rediris.es/difusion/publicaciones/boletin/76/enfoque2.pdf