Procedimientos de Seguridad Básicos

Antonio Yáñez Izquierdo

Octubre 2011

Procedimientos de Seguridad Básico

Procedimientos de Seguridad Básicos

- En la seguridad de un equipo informático distinguimos dos vertientes
  - **Seguridad física:** Seguridad de los elementos físicos constitutivos del equipo: *hardware*
  - **Seguridad de la información** Seguridad de la información almacenada en el equipo informático: software y archivos de datos. Podemos considerar dos aspectos
    - Seguridad de la información propiamente dicha
    - Protección contra accesos indebidos

Seguridad física I

- El objetivo es mantener los equipos en perfecto estado de funcionamiento el mayor tiempo posible. Para ello, debemos tener en cuenta que se trata de un equipo delicado. Algunas recomendaciones
  - Tratar el equipo con cuidado, no forzando los movimientos (de apertura, cierre o rotación de la pantalla) ni haciendo fuerza de partes frágiles (por ejemplo, no tirar de la cámara para abrir la pantalla)
  - Usar el puntero original para el manejo de la pantalla tactil. El uso de otros dispositivos (con diferente dureza y/o tamaño) puede dañar la pantalla
  - Mantener siempre la batería en posición de bloqueo, para evitar que se pueda desconectar bruscamente
  - Usar los conectores adecuados y no forzar su entrada y/o salida en los receptores del equipo (los conectores deben entrar y salir con suavidad, nunca de manera forzada).
    - Algunos de ellos tienen un sistema de enclavamiento (por ejemplo el de la tarjeta de red) que es necesario liberar antes de retirar el conector.

Seguridad física II

- El conector VGA de 15 pines tiene tendencia a doblar alguno de los pines si no se introduce correctamente
- No obstruir las tomas de ventilación del equipo.
  - El equipo tiene unas necesidadesd e refrigeración reales.
  - Suele venir configurado de manera que al llegar a cierta temperatura de funcionamiento se apaga automáticamente
  - El uso continuado por encima de su temperatura de funcionamiento puede dañar algunos componentes
- No retirar dispositivos tales como discos duros externos cuando están siendo accedidos
  - El corte repentino de la la alimentacion siministrada por el conector USB podría producir daños físicos

Seguridad de la información

- Toda la información almacenada en nuestro sistema es susceptible de perderse ante un fallo del hardware
  - Debemos tener una política de copias de seguridad
- Debemos cerrar las aplicacionenes antes de cerrar el sistema
- El sistema debe apagarse con la opción de *apagar sistema*, Esto hace que todos los procesos del sistema se detengan ordenadamente, impidiendo la pérdida de datos (normalmente al pulsar el botón de apagado iniciamos el procedimiento ordenado de apagar el sistema, pero no siempre es así)
  - En ninguna circunstancia debe cortarse la alimentacion del sistema (retirarle la batería) mientras está funcionando: podría dejar el sistema de ficheros en un estado inconsistente y no poder arrancar de nuevo
- La unidades extraibles deben retirarse con el procedimiento de *desmontar*, *expulsar* o *retirar de forma segura*. De no hacerse así podrían perderse datos

Protección contra accesos indebidos

- Se consideran accesos indebidos, tanto los accesos a nuestros datos como la utilización de nuestro equipo (y/o identidad) para acceder a datos (o equipos) de otros. Hay una serie de consideraciones a tener en cuenta
  - Nunca utilizar una cuenta con privilegios de *administrador* para trabajar en el sistema. Usar los privilegios de administrador solo para realizar las tareas de administración.
    - Existe la tendencia a usar cuentas con privilegios de administrador en los sistemas *windows*. Esto hace que un error (o un virus) pueda comprometer todo el sistema
    - Nuestro usuario en los equipos abalar no tiene privilegios de administrador, por lo que lo único que podemos comprometer son nuestros datos

Protección contra accesos indebidos

- No utilizar contraseñas como *qwerty*, *1234* . . . en las distintas entidades donde tengamos cuenta
- No pulsar en enlaces que aparecen en correos y de cuya veracidad no estamos seguros
- No enviar contraseñas a los correos que nos las piden (*phishing*)
- No ejecutar programas cuya procedencia desconocemos.

Actividades

- Insertar un cable de red y comprobar el enclavamiento
- Usar el editor de texto *gedit* para crear un texto de 20 lineas. Intentar cerrar el editor sin salvar el texto
- Intentar apagar el sistema sin haber guardado el texto
- Copiar varios archivos (uno de ellos de buen tamaño) a una unidad extraible, retirarla inmediatamente en cuanto haya desaparecido la barra de progreso
  - Volver a insertarla y comparar los arcivos original y copia
- Copiar un fichero de texto a una unidad extraible. Abrir el fichero desde la unidad extraible. Retirar la unidad extraible directamente