



Buenas prácticas de seguridad





electrónico, disco flexible, memoria usb, cd-rom), se analice con un antivirus, el cual debe estar actualizado con las definiciones más recientes de virus.

Si no se cuenta con antivirus instalado en tu equipo, existen versiones de antivirus que realizan un análisis en línea, con los cuales puedes revisar el equipo o determinadas partes del equipo.

Para mayor información puedes consultar: **Software Antivirus**

Establece una contraseña compleja en tu equipo

La mayoría de las veces no basta con tener un firewall, un antivirus y un antispyware, debido a que los intrusos cuentan también con técnicas para atacar a tu equipo con solo conocer el nombre de usuario y la contraseña del mismo.

Hoy en día es muy común que los equipos tengan contraseñas débiles, lo que representa un riesgo de seguridad alto. Esta mala configuración de contraseñas por lo general tiene los siguiente defectos:

Contraseñas en blanco, es decir, no utilizar una contraseña para entrar al equipo.

seguridad de usuarios. Una
contraseña fuerte debe cumplir con las siguientes características:
8 dígitos 0-9, 3 letras mayúsculas y 2 minúsculas.



Ahora por último solo nos falta agregar símbolos para lo cual se puede cambiar una "s" por "\$", una "y" por "&" o una "a" por una "@" y la frase terminaría de esta manera: "\$0yUn1v3rs1t@rio" que ya es una contraseña fuerte.

Otra técnica es el uso de la passphrase. Para esta técnica se utilizan frases comunes o cosas personales fáciles de recordar. Como por ejemplo: "El Congreso de Seguridad se ha celebrado 11 veces", algo largo pero más fácil de recordar que 32x!Ewzmsc. Otro ejemplo sería "La comida es a las 14 horas".

Si a todo esto le combinamos el cambiar letras por números o símbolos como lo habíamos mencionado anteriormente nos quedaría una contraseña aun más fuerte y difícil de romper como es : "L@ c0mida 3s a las 14 hor4s".

Finalmente se recomienda que las contraseñas sean cambiadas después de un determinado tiempo, además de utilizar contraseñas diferentes para cada servicio que utilices.

No reveles tu contraseña a ninguna persona extraña

Debes tomar en cuenta que una contraseña fuerte deja de ser fuerte cuando alguien más la conoce. Es muy importante que la contraseña sea confidencial para lo cual es necesario que no se comparta con ninguna otra persona, no se escriba en un post-it, una libreta, debajo del teclado o en algún otro sitio.

Lo anterior se debe a que es común del txista gente mal intencionada que al tener una contraseña en su poder, realice acciones no éticas en los equipos. Estas acciones pueden ser el borrar, modificar o copiar información, instalar programas del afecten la seguridad de nuestra información o del capturen contraseñas de otras cuentas. En el peor de los casos, un usuario podría utilizar la contraseña para realizar actividades mal2n dsporrnastae
