# Reflexiones por capítulo

Algunas reflexiones del curso que me quedan son de actualizar mis conocimientos de forma regular y brindar protección a mis aplicaciones y datos personales.:

* Actualice regularmente su sistema operativo y el software instalado en su equipo, poniendo especial atención a las actualizaciones de su navegador web. Estar al día con las actualizaciones, así como aplicar los parches de seguridad recomendados por los fabricantes, le ayudará a prevenir la posible intrusión de hackers y la aparición de nuevos virus.
* Instale un Antivirus y actualícelo con frecuencia. Analice con su antivirus todos los dispositivos de almacenamiento de datos que utilice y todos los archivos nuevos, especialmente aquellos archivos descargados de internet.
* Instale un Firewall o Cortafuegos con el fin de restringir accesos no autorizados de Internet.
* tilice contraseñas seguras, es decir, aquellas compuestas por ocho caracteres, como mínimo, y que combinen letras, números y símbolos. Es conveniente además, que modifique sus contraseñas con frecuencia. En especial, le recomendamos que cambie la clave de su cuenta de correo si accede con frecuencia desde equipos públicos.
* Navegue por páginas web seguras y de confianza. Para diferenciarlas identifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. Extreme la precaución si va a realizar compras online o va a facilitar información confidencial a través de internet
* Ponga especial atención en el tratamiento de su correo electrónico, ya que es una de las herramientas más utilizadas para llevar a cabo estafas, introducir virus, etc.
* No abra mensajes de correo de remitentes desconocidos.
* Desconfíe de aquellos e-mails en los que entidades bancarias, compañías de subastas o sitios de venta online, le solicitan contraseñas, información confidencial, etc.
* No propague aquellos mensajes de correo con contenido dudoso y que le piden ser reenviados a todos sus contactos. Este tipo de mensajes, conocidos como hoaxes, pretenden avisar de la aparición de nuevos virus, transmitir leyendas urbanas o mensajes solidarios, difundir noticias impactantes, etc.
* En general, es fundamental estar al día de la aparición de nuevas técnicas que amenazan la seguridad de su equipo informático, para tratar de evitarlas o de aplicar la solución más efectiva posible.

Fernando Cutire