

Mapa conceptual / Interactividad

**Buenas prácticas de seguridad informática**

* **Mantener actualizado el sistema operativo, los antivirus y las aplicaciones:** Las últimas versiones traen incluidas no solo las últimas herramientas sino también los más recientes parches de seguridad.
* **Asegurar el sistema operativo:** Es fundamental tener asegurados algunos elementos del sistema operativo como deshabilitar las carpetas compartidas, utilizar contraseñas fuertes, restringir los privilegios de los usuarios, deshabilitar la ejecución automática de dispositivos USB, entre otros.
* **Protección del correo electrónico:** El correo electrónico es uno de los medios más utilizados para propagar virus y malware, por lo tanto es necesario tener algunos cuidados como: no descargar archivos adjuntos en correos de usuarios desconocidos, utilizar filtros anti-spam; tener en cuenta que los bancos y entidades financieras no solicitan datos confidenciales a través de este medio, así que nunca se debe enviar números y claves de tarjetas de crédito, y ni seguir enlaces (links), adjuntos en estos correos.
* **Seguridad en la navegación web:** evitar los sitios web que son ilegales, como los que ofrecen cracks, ya que por ellos pueden llegar archivos malware; instalar un antivirus que incluya protección web, impedir la ejecución de archivos desde sitios web sin verificar su autenticidad; descargar programas solamente del sitio oficial del mismo, para evitar que hayan sido manipulados y alterados por terceros; si se navega en sitios públicos hacer navegación de incógnito, para no dejar huella de los sitios visitados y las actividades realizadas en ellas.
* **Seguridad en redes sociales:** configurar el perfil para que no sea público, así se logra mantener la privacidad; no publicar información sensible y confidencial; no aceptar solicitudes de desconocidos ya que pueden contener códigos maliciosos; ignorar los mensajes que contienen material pornográfico, ya que a través de ellos se suele hacer propagación de malware, además de ser ofensivos desde el punto de vista ético y moral; evitar subir fotografías propias y de la familia, ya que pueden servir para identificarte a ti y a tus familiares cercanos para cometer actos delictivos como extorsiones y secuestro; se recomienda cambiar la contraseña periódicamente, para evitar que sea descubierta fácilmente.
* **Seguridad en redes P2P:** las redes punto a punto son blanco constante de ataques debido a que todos los nodos son igualitarios; por eso se debe evitar almacenar información sensible y confidencial en la misma computadora en la que se comparte archivos, para evitar que esta sea copiada; utilizar un antivirus confiable que analice todos los archivos que se descargan sin importar la extensión; impedir que el programa cliente de intercambio de archivos no instale componentes adicionales, ya que en la mayoría de los casos pueden ser códigos maliciosos; verificar la coherencia entre el tamaño del archivo original y el descargado, porque podría cotener troyanos.
* **Seguridad en mensajería instantánea:** es otro de los medios más utilizados en la actualidad y por lo tanto uno de los mas atractivos para los cyberdelincuentes, los cuidados que se deben tener son similares a los del correo electrónico; no descargar archivos sospechosos; en caso de descargar archivos, explorarlos con un antivirus, no seguir enlaces incrustados, ya que pueden llevar a páginas con contenido malicioso o descargas de malware; no descargar archivos de usuarios desconocidos. Además se debe evitar aceptar contactos con cuentas desconocidas sin verificar a quién pertenece; no intercambiar información confidencial ya que estas comunicaciones pueden ser interceptadas y la información utilizada para fines delictivos.
* **Seguridad en dispositivos removibles:** estos dispositivos que se conectan a puertos USB (memorias, cámaras, celulares, etc), son una de las mayores fuentes de propagación e infección de malware; algunas de las medidas a tener en cuenta son: establecer lineamientos que indiquen el uso correcto del dispositivo removible, ya que podrían servir como medio de transporte de códigos maliciosos o para extraer información de los computadores; si se almacena información confidencial en ellos, se debe hacer cifrado. Esto evita que en caso de robo o extravío, la información no pueda ser vista por terceros; configurar el antivirus para que analice cualquier dispositivo tan pronto este se conecte y de ser necesario lo bloquee, para evitar una posible infección; deshabilitar la ejecución automática en el sistema operativo Windows; en casos extremos, tener los puertos bloqueados.