



## 1. ¿Son seguros los equipos públicos o compartidos?

- a) Sí, está claro que todos los equipos están configurados para ese tipo de uso, y es mantenido por gente formada y que tiene amplios conocimientos de causa.
- b) No, nunca debemos fiarnos de estos equipos debido a que no sabemos qué intenciones han podido tener otros usuarios o si no tienen conocimiento de causa.
- c) No, no es seguro ejecutar ficheros desde ellos, pero si lo es la navegación en la red, por lo que es posible usarlo con información de tipo privado.

## 2. ¿Cuáles son las dos fuentes de vulnerabilidades en un equipo público?

- a) El local donde se ubique (ciber-cafés, locutorios,..) y la ausencia de salvapantallas.
- b) El propio equipo y el local donde se ubique (ciber-cafés, locutorios,..).
- c) El propio equipo y las redes de comunicación a las que está conectado.

## 3. ¿En qué momentos se puede hacer uso de equipos públicos?

- a) Nunca, en ningún caso.
- b) Sólo si no existe otra opción y se está seguro que no se van a usar datos confidenciales o personales.
- c) Siempre, pero manteniendo la precaución de tener activado el salvapantallas.

## 4. ¿Es necesario salvar los ficheros que hayamos creado, con información confidencial, cuando dejemos un PC público?

- a) No existe ningún criterio específico, ya que no afecta a la seguridad.
- b) Sí, hay que asegurarse que quedan salvados antes de dejar la sesión.
- c) No hay que dejar ningún fichero con esa clase de información ni de otro tipo.

## 5. ¿En qué momento puede considerarse seguro el uso de un PC compartido?

- a) Nunca, en todo momento hay que tener en cuenta las precauciones en su uso.
- b) Sólo en el momento en que el equipo esté totalmente actualizado, tanto en las aplicaciones como en el Sistema Operativo.
- c) Siempre es posible usar un equipo compartido con seguridad.

# RESPUESTAS.Precauciones en el uso de equipos públicos o compartidos



Nº Pregunta	Respuesta
1	B
2	C
3	B
4	C
5	A