1. ¿Son más seguros los PCs públicos que los propios?

a) No, los riesgos a los que nos exponemos en ellos son mucho mayores dado que no disponemos de ningun control para aplicar medidas de seguridad sobre ellos.

b) No, los propios por defecto siempre están mucho más securizados.

c) Sí, al ser públicos y empleados por varios usuarios, tenemos muchos más puntos de vista para conseguir un medio más seguro.

2. ¿Es fiable y seguro conectarse para ver información personal y confidencial en PCs públicos?

a) Sí, como en cualquier PC los riesgos son bajos si está conectado a una red con contraseña.

b) Sí, siempre que al conectarme a ver dicha información utilice protocolos seguros como https que me asegurará que nadie pueda conseguir mi información.

c) No, de ningún modo. No podemos saber quién y de qué modo ha usado el PC anteriormente y si este ya está infectado O posee algún tipo de malware.

3. ¿Es crítico instalar un software de procedencia desconocida?

a) No, tengo antivirus actualizado asi que no corro riesgos instalandolo porque me avisaría si hubiera cualquier amenaza.

b) No, puesto que lo he bajado de una página que me asegura que está libre de virus.

c) Sí, a pesar de tener antivirus u otros sistemas de protección instalados, nunca se puede estar completamente seguro del software que no es de procedencia fiable.

4. Siempre que puedo uso el usuario con mayor número de privilegios posibles para no tener que andar cambiando si necesito algún permiso extra, ¿actúo bien?

a) Sí.

b) No.

5. ¿Conectarse a una red wifi pública conlleva algún riesgo?

a) No, aunque me conecte a una red wifi sin contraseña, esta tiene que disponer de las medidas de seguridad necesarias para que no me preocupe mi seguridad.

b) Sí, pero no me preocupa porque tengo antivirus, firewall,... y nadie puede llegar a mi información.

c) Sí, a pesar de tener antivirus, firewall... siempre existen riesgos.

6. ¿Cuál es el malware más problematico y perjudicial para un sistema?

a) El que está continuamente sacandote mensajes molestos y no te deja en paz.

b) El que se instala y corrompe poco a poco tu sistema gastando recursos y ralentizándolo.

c) El que se instala, trata de pasar inadvertido y recopila la mayor cantidad de infomación posible sin que el usuario pueda apreciar ningún cambio en la funcionalidad del sistema.

7. ¿Cómo de importante es mantener los sistemas (sistema operativo, antivirus, etc...) actualizados?

a) No es tan importante, sólo si pasas más de 15 días sin actualizarlo.

b) Un sistema desactualizado es siempre un sistema de alto riesgo.

c) Es muy importante pero no importa que no lo estén si se dispone de muchos sistemas de defensa instalados (antivirus, firewall, antispyware, etc...).

8. Me han recomendado que desinstale algún servicio que no uso de mi sistema, pero como dispongo de muchos sistemas de defensa instalados, no lo veo necesario. ¿Estoy en lo cierto?

a) Sí, estando actualizados y con esas medidas defensivas no hay riesgo alguno.

b) No, aún actualizado y con esas medidas de seguridad existen protocolos que dada su implementación presentan graves deficiencias de seguridad y es recomendable su desinstalación.

c) Sí, cualquier servicio instalado en el sistema es seguro.

9. ¿Es recomendable el uso de un entorno de prueba si se duda de la procedencia de un fichero o url?

a) No, si tenemos un sistema seguro y actualizado no hay riesgo de infección.

b) Sí, la ejecución de ficheros o urls de dudosa procedencia es un riesgo importante de seguridad, lo mejor es no ejecutarlo, o ejecutarlo primero en un entorno controlado donde no tengamos información relevante ni acceso a otros sistemas que podamos dañar.

10. ¿Es seguro tener habilitado el servicio telnet o ftp?

a) Sí, son protocolos seguros.

b) No, poseen ciertas deficiencias y cuando no se necesitan, por seguridad deberían estar deshabilitados.

Nº Pregunta	Respuesta
1	A
2	C
3	C
4	B
5	C
6	C
7	B
8	B
9	B
10	B