1. ¿Son máis seguros os PCs públicos que os propios?

a) Non, os riscos ós que nos expoñemos en eles son moito maiores dado que non dispoñemos de ningún control para aplicar medidas de seguridade sobre eles.

b) Non, os propios por defecto sempre están moito máis securizados.

c) Si, ó ser públicos e empregados por varios usuarios, temos moitos máis puntos de vista para conseguir un medio máis seguro.

2. ¿É fiable e seguro conectarse para ver información persoal e confidencial en PCs públicos?

a) Si, como en calquera PC os riscos son baixos se está conectado a unha rede con contrasinal.

b) Si, sempre que ó conectarme a ver dita información empregue protocolos seguros como https que me asegurará que ninguén poida conseguir a miña información.

c) Non, de ningún modo. Non podemos saber quen e de que modo foi usado o PC anteriormente e se este xa está infectado Ou posúe algún tipo de malware.

3. ¿É crítico instalar un software de procedencia descoñecida?

a) Non, teño antivirus actualizado asi que non corro riscos instalando porque me avisaría se houbera calquera ameaza.

b) Non, posto que o baixei dunha páxina que me asegura que está libre de virus.

c) Si, a pesar de ter antivirus ou outros sistemas de protección instalados, nunca se pode estar completamente seguro do software que non é de procedencia fiable.

4. Sempre que podo uso o usuario con maior número de privilexios posibles para non ter que andar cambiando se preciso algún permiso extra, ¿actúo ben?

a) Si.

b) Non.

5. ¿Conectarse a unha rede wifi pública conleva algún risco?

a) Non, aínda que me conecte a unha rede wifi sen contrasinal, esta ten que dispoñer das medidas de seguridade necesarias para que non me preocupe a miña seguridade.

b) Si, pero non me preocupa porque teño antivirus, firewall,... e ninguén pode chegar á miña información.

c) Si, a pesar de ter antivirus, firewall... sempre existen riscos.

6. ¿Cal é o malware máis problematico e perxudicial para un sistema?

a) O que está continuamente sacando mensaxes molestos e non te deixa en paz.

b) O que se instala e corrompe pouco a pouco o teu sistema gastando recursos e ralentizando.

c) O que se instala, trata de pasar inadvertido e recopila a maior cantidade de infomación posible sen que o usuario poida apreciar ningún cambio na funcionalidade do sistema.

7) ¿Como de importante é manter os sistemas (sistema operativo, antivirus, etc...) actualizados?

a) Non é tan importante, só se pasas máis de 15 días sen actualizalo.

b) Un sistema desactualizado é sempre un sistema de alto risco.

c) É moi importante, pero non importa que non o estén se se dispón de moitos sistemas de defensa instalados (antivirus, firewall, antispyware, etc...).

8. Recomendaronme que desinstale algún servizo que non uso do meu sistema, pero como dispoño de moitos sistemas de defensa instalados, non o vexo necesario. ¿Estou no certo?

a) Si, estando actualizados e con esas medidas defensivas non hai risco algún.

b) Non, aínda actualizado e con esas medidas de seguridade existen protocolos que dada a súa implementación presentan graves deficiencias de seguridade e é recomendable a súa desinstalación.

c) Si, calquera servizo instalado no sistema é seguro.

9. ¿É recomendable o uso dun entorno de proba se se duda da procedencia dun ficheiro ou url?

a) Non, se temos un sistema seguro e actualizado non hai risco de infección.

b) Si, a execución de ficheiros ou urls de dubidosa procedencia é un risco importante de seguridade, o mellor é non executalo, ou executalo primeiro nun entorno controlado onde non teñamos información relevante nin acceso a outros sistemas que poidamos dañar.

10. ¿É seguro ter habilitado o servizo telnet ou ftp?

a) Si, son protocolos seguros.

b) Non, poseen certas deficiencias e cuando non 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