Plantillas de cuestionarios de sensibilización

para padres y madres,usuarios finales y PYME

enisa
European Network and Information Security Agency

Acerca de ENISA

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) ha sido creada con el objetivo de impulsar el funcionamiento del mercado interior. ENISA es un centro de excelencia para la seguridad de las redes y la información de los Estados miembros europeos e instituciones europeas, que ofrece asesoramiento y recomendaciones y funciona a modo de centralita de información sobre buenas prácticas. Además, la agencia facilita contactos entre las instituciones europeas, los Estados miembros y los agentes de la industria y la empresa privada.

Información de contacto

A continuación se facilita la información para ponerse en contacto con ENISA o para realizar cualquier consulta sobre cuestiones relacionadas con la sensibilización sobre la seguridad de la información:

Correo electrónico: KJELL KALMELID, experto en sensibilización — kjell.kalmelid@enisa.europa.eu

Internet: http://www.enisa.europa.eu

Agradecimientos

Kjell Kalmelid, experto en sensibilización, ENISA y coordinador de este documento, desea expresar su más sincero agradecimiento a los cuatro autores de la Comunidad «sensibilización» que han trabajado juntos en la elaboración y recopilación de las plantillas del cuestionario:

- Anna Rywczyñska, NASK, Polonia
- Pierre-Luc Refalo, Hapsis Education, Francia
- Claudio Telmon, CLUSIT, Italia
- Johannes Wiele, Konradin IT-Verlag y Ludwig-Maximilians-Universität Munich, Alemania

También quiere manifestar su especial agradecimiento a Peter Pfeifhofer, experto nacional en comisión de servicio de ENISA y a Wendy Goucher, Idrach Ltd., Reino Unido y miembro de la Comunidad «sensibilización» por revisar las plantillas y ofrecer sus opiniones.

Índice

Preámbulo

Acerca de este documento

Este documento es el resultado del trabajo conjunto de cuatro miembros de la Comunidad «sensibilización» de ENISA. Su objetivo es ofre cer información acerca de la sensibilización sobre la seguridad de la información en la forma de una serie de plantillas de un cuestionario.

Acerca de la Comunidad «sensibilización»

La Comunidad «sensibilización» es una comunidad de inscripción gratuita abierta a profesionales que trabajan en el ámbito de la seguridad de la información. Fue puesta en marcha en 2008 por ENISA a fin de crear una comunidad centrada en la seguridad de la información, destinada especialmente a profesionales interesados en cuestiones de sensibilización sobre seguridad.

A pesar de que la Comunidad «sensibilización» está dirigida principalmente a los miembros europeos, cuenta también con varios miembros de países de fuera de Europa que comparten la misma idea: la importancia clave de sensibilizar a la sociedad sobre la seguridad con el fin de lograr un auténtico estado de seguridad de la información en cualquier organización.

Introducción

Ámbito de aplicación

El objetivo de este documento es ofrecer información en torno a la sensibilización sobre la seguridad de la información en la forma de una serie de plantillas de un cuestionario. Este documento está dirigido a las organizaciones que desean sensibilizar sobre la seguridad de la información entre sus grupos destinatarios.

Objetivo

Estos cuestionarios no deberían considerarse exámenes completos para conocer el nivel de sensibilización y el grado de conocimiento de las personas. El objetivo no es otro que ayudar a la persona que responde a tener una idea de su nivel de sensibilización y, en el mejor de los casos, ofrecerle una herramienta para despertar su interés sobre los valores y los riesgos de utilizar ordenadores y servicios en línea en Internet.

Cómo utilizar las plantillas

Las plantillas pueden utilizarse bien impresas con una hoja de respuestas o bien como un cuestionario en la red. Cada cuestionario tiene una *introducción* que deberá guardarse o, si se cuelga en Internet, deberá incluirse en la misma página que las preguntas.

IMPORTANTE

Además de la información ofrecida en las columnas «Comentarios», deberán incluirse fuentes nacionales o locales de información que puedan ser importantes, como enlaces, información de contacto a líneas directas y autoridades locales/nacionales. En algunas preguntas esto se indica entre corchetes, por ejemplo [INSERTAR PUNTO DE CONTACTO PERTINENTE].

Estructura de los cuestionarios

En total hay tres tipos de cuestionarios, cada uno destinado a un grupo diferente: padres y madres, usuarios y directores ejecutivos de pequeñas y medianas empresas (PYME).

Cada plantilla consta de una serie de *temas* divididos en *preguntas* que, a su vez, están seguidas de una columna con *Comentarios*. En algunos cuestionarios, los comentarios pueden contener información correcta e incorrecta junto con texto informativo y a veces sólo información breve.

Padres y madres

Tema	Preguntas	Comentarios
Utilización que su hijo hace del ordenador	1. Actividades en línea 2. Comunicación 3. Utilización del PC 4. Internet y riesgos 5. Conocimiento de Internet	Permite a los progenitores saber hasta qué punto sus hijos deberían utilizar el ordenador y para qué actividades

Privacidad y plataformas de comunicación electrónicas	6. Utilizar plataformas de comunicación electrónicas 7. Crear perfiles seguros 8. Revelar información	Permite saber a los progenitores cómo crear perfiles seguros, si sus hijos tienen un perfil en línea, qué información no deberían colgar
Contenidos ilícitos	9. Informar si se encuentran contenidos ilícitos 10. Localizar contenidos ilícitos	Software de filtrado: ¿sabe cómo usarlo?
Compartir archivos	11. Utilizar tecnología de par a par	Los niños descargan archivos multimedia. ¿Los progenitores conocen la legislación sobre derechos de autor? ¿Qué está permitido y qué no?
Acoso cibernético (o *cyber-bullying*)	12. Reaccionar frente al acoso cibernético	¿Qué consecuencias tiene publicar información falsa y/o acosar a alguien en Internet?

Usuarios finales

Tema	Preguntas	Comentarios
Amenazas en Internet	1. Archivos adjuntos en mensajes 2. Programas antivirus y cortafuegos 3. Actualizaciones de parches/seguridad 4. Contraseñas	¿La persona que responde conoce las diferentes amenazas y sabe cómo protegerse de ellas?
Phishing	5. Compra segura en línea 6. Conocer el *phishing*	¿La persona que responde sabe cómo comprar con seguridad en Internet y está al tanto de la amenaza de los ataques de *phishing*?
Protección de la información	7. Copia de seguridad 8. Memorias USB 9. Conocer el cifrado	¿La persona que responde conoce la importancia de hacer copias de seguridad de la información importante, conoce los riesgos y las desventajas de las memorias USB y el cifrado para proteger la información?

Aspectos legales/derechos de autor	10. Descarga de archivos	¿Cuál es la diferencia entre Internet y el mundo real? Descarga de material con derechos de autor

PYME

Tema	Preguntas	Comentarios
Perfil de riesgo	1. Activos de información 2. Amenazas	Los directivos de PYME deberán identificar la información clave y las posibles amenazas
Temas contractuales y legales	3. Privacidad/datos personales 4. Licencias de software 5. Gestión de los contratos	Los directivos de PYME deberán conocer estas responsabilidades legales.
Aspectos humanos y organizativos	6. Gestión de la contraseña 7. Correo electrónico 8. Navegar en Internet 9. Ingeniería social 10. Dispositivos portátiles	Deberán adoptarse ciertos comportamientos para reducir los riesgos relacionados con el acceso y las comunicaciones. Los directivos deberán dar ejemplo a sus empleados.
Herramientas de seguridad	11. Copia de seguridad 12. Antivirus/*spyware* 13. Acceso remoto seguro 14. Cifrado	Ciertas tecnologías son necesarias para proteger los sistemas de información y los datos confidenciales. Los directivos de PYME deberán conocer cuál es la línea base de seguridad que han que implementar.

Cuestionario para padres y madres

Cuestionario para padres y madres

Introducción al perfil de cuestionario para padres y madres

Le damos la bienvenida al cuestionario de sensibilización ENISA para padres y madres!

El objetivo de este cuestionario es ofrecerle, como progenitor, una herramienta para comprobar su nivel de sensibilización y grado de conocimiento sobre una serie de temas en relación con el uso que su hijo/a hace del ordenador y de los servicios en línea de Internet.

Internet es una herramienta fantástica que ofrece abundante y valiosa información y servicios. Sin embargo, también tiene algunos riesgos, y como padre o madre, debería conocerlos.

No pretendemos que estas preguntas sean un test completo para conocer su nivel de sensibilización y grado de conocimiento. El objetivo no es otro que ayudarle a tener una idea de su nivel de sensibilización y, en el mejor de los casos, ofrecerle una herramienta para despertar su interés sobre los valores y los riesgos que comporta el hecho de que su hijo/a utilice Internet. También esperamos que las fuentes de información que se ofrecen en este sitio web le sean de utilidad.

Nº	Pregunta	Respuestas	Comentarios
1	¿Cuáles son las actividades en línea de su hijo/a?	a) Chatear o comunicarse por correo electrónico b) Mantener un blog o utilizar plataformas de comunicación electrónica c) Jugar a juegos de ordenador en línea d) Buscar información en Internet para hacer los deberes o trabajos del colegio e) Todos los anteriores, más o menos f) No lo sé	f) Se recomienda que los progenitores estén al tanto de las actividades que los hijos realizan en línea. Pregúnteles a sus hijos qué están haciendo, y pídales que le enseñen cómo funcionan las diferentes funciones, juegos u otras actividades en línea. De este modo, su hijo/a entenderá que tiene interés real en lo que él/ella está haciendo. También es importante que sepa si su hijo/a está realizando alguna actividad que considera fuera de los límites permitidos. a)-e) Parece que su hijo/a saca provecho de las ventajas de la TI. Está muy bien. Parece además que sabe lo que su hijo/a está haciendo cuando utiliza el ordenador (en principio, cuantas más casillas cubra, más sabe). **Consejos básicos** Coloque el/los ordenador/es de la casa en sitios bien visibles, como salas comunes o la cocina, para poder controlar fácilmente las actividades de los niños.
2	¿Habla con su hijo/a sobre las actividades que realiza en Inter-	a) Sí b) No	a) y c) Es muy bueno hablar de estos temas con los niños. Continúe haciéndolo regular-

Nº	Pregunta	Respuestas	Comentarios
	net?	c) A veces	mente. b) Es muy importante hablar periódicamente estos temas con su hijo/a. Básicamente, es el único modo de saber qué actividades hace su hijo/a en línea y de poder conocer los posibles riesgos. **Consejos básicos** La confianza es fundamental. Mantenga las vías de comunicación abiertas para que sus hijos hablen de sus actividades en línea y al mismo tiempo sientan que cuentan con su aprobación para explorar Internet de forma responsable
3	Por término medio, ¿cuánto tiempo dedica su hijo/a a utilizar el ordenador?	a) Más de 3 horas al día b) Entre 2 y 3 horas al día c) Entre 1 y 2 horas al día d) Todo el tiempo que necesita e) No lo sé f) Menos de 1 hora al día	a) – e) Asegúrese de que sabe cuánto tiempo al día dedica su hijo/a al ordenador. No olvide que su hijo/a también tiene que hacer deporte u otra actividad física. f) Menos de 1 hora al día no es preocupante. **Consejos básicos** Si su hijo/a dedica demasiado tiempo a jugar o a utilizar servicios en línea, especialmente por la noche, debería ser una señal para considerar la posibilidad de restringir el uso del ordenador de su hijo/a.
4	¿Cree que Internet supone un	a) No, los riesgos están sobreestimados	a) Es cierto que a veces se concede excesiva

Nº	Pregunta	Respuestas	Comentarios
	riesgo?	b) Sí, mucho c) Hay riesgos, pero también herramientas de comunicación, servicios e información útil d) No lo sé	importancia a los riesgos, pero también es difícil evaluarlos porque continuamente se están introduciendo nuevos servicios y funciones en Internet. b) y c) Está bien que sea consciente de que Internet puede resultar peligroso para su hijo/a, pero no olvide que también es una herramienta de comunicación y que ofrece servicios e información útil. d) Lo mejor que puede hacer es intentar aprender tanto como pueda sobre los riesgos de Internet y, para empezar, seguir las recomendaciones de seguridad de su proveedor de servicios en este sitio web.
5	¿Hasta qué punto cree que sabe utilizar Internet?	a) Mejor que mi hijo/a b) Más o menos como mi hijo/a c) Peor que mi hijo/a d) No lo sé	a) y c) Está bien que sepa qué nivel tiene en comparación con su hijo/a. De nuevo, es importante que procure saber más sobre los riesgos en línea y sobre cómo evitarlos. c) No se sienta desconcertado por el hecho de que su hijo/a parezca saber mucho más sobre Internet y los servicios que ofrece que usted. Muchos padres y madres están en la misma situación. d) Si no lo sabe, le recomendamos sentarse de

Nº	Pregunta	Respuestas	Comentarios
			vez en cuando con su hijo/a y navegar con él/ella por la web. Enseguida tendrá la respuesta.
6	¿Qué información puede revelar su hijo/a sin riesgos cuando utiliza plataformas de comunicación electrónica?	a) El nombre real y sólo la inicial del apellido b) El nombre de su colegio c) Su color favorito d) Los nombre reales de sus padres, pero no los suyos e) La fecha de nacimiento, pero no el nombre f) Nombres de amigos o parientes g) Su apodo	a), b), c), d) y f) - Incorrecto. Deberá explicarle a su hijo/a que nunca ha de revelar ninguna información en Internet que permita que alguien lo/la identifique en la vida real. c) y g) Correcto. Un apodo o un color favorito es información segura en Internet.
7	¿Su hijo/a ha creado un perfil seguro en la plataforma de comunicación electrónica que utiliza?	a) Sí b) No c) No lo sé d) Mi hijo/a no usa ninguna plataforma de comunicación electrónica	a) ¡Bien! De todas formas, compruebe que su hijo/a sabe utilizar las plataformas de comunicación electrónicas de forma segura. Asegúrese de que el perfil seguro de su hijo/a cumple las recomendaciones básicas que se ofrecen más adelante. b) Siga los consejos básicos que se ofrecen más adelante para crear un perfil seguro para su hijo/a. c) Al no saber cómo utilizar las plataformas de comunicación electrónicas de forma segura se podría violar la privacidad de su hijo/a. d) Este tipo de plataformas son muy utilizadas entre los niños y los adolescentes. Pueden ser una herramienta muy útil y divertida, por ejemplo, para estar en contacto con

Nº	Pregunta	Respuestas	Comentarios
			amigos de todo el mundo. **Consejos básicos para crear perfiles seguros:** 1. Configure su perfil como privado para permitir que otros usuarios sólo vean el nombre de usuario de su hijo/a, y si desea colgar cualquier otra información, por ejemplo, una foto de su hijo/a, hágalo con acceso restringido. Permita que sólo los amigos de su hijo/a puedan acceder a la información adicional. Asegúrese de que conoce a los amigos de su hijo/a. 2. Nunca ponga en línea datos privados como el nombre real, la dirección, fotos o números de teléfono. 3. Sea selectivo con las fotos. Una vez en línea, quedarán en Internet para siempre. Respete la privacidad de otros: no deje que su hijo/a cuelgue fotos de otras personas sin pedir permiso. 4. Dígale a su hijo/a que les diga a sus amigos que creen perfiles seguros. No dude en hablar de estos temas con los padres de los amigos de su hijo/a.

Nº	Pregunta	Respuestas	Comentarios
8	¿Qué información puede revelar si quiere crear un perfil seguro en una plataforma de comunicación electrónica?	a) Puedo dar mi número de teléfono, pero no mi dirección de correo electrónico b) Puedo dar mi dirección postal, pero no mi número de teléfono c) Puedo decirles a las personas con las que me relaciono en línea dónde trabajo o a qué colegio voy d) Puedo revelar cualquier información personal a personas en las que confío e) Puedo colgar una foto mía siempre y cuando no revele ninguna información personal sobre mí	a) - c) Este tipo de información es un ejemplo de datos privados. No debería poner ninguna información personal en línea. Sin embargo, si decide hacerlo, asegúrese de que sólo las personas de su confianza pueden acceder a ella. d) No debería colgar ninguna información personal en línea. Haga su perfil privado y asegúrese de que sólo las personas de su confianza tienen acceso. Puede usar su apodo en las plataformas de comunicación electrónicas, siempre y cuando no añada ninguna otra información que pueda revelar su identidad. e) Una foto suya es información personal.
9	¿Sabe a quién debería informar si encuentra contenidos ilícitos en Internet? Una o más preguntas son correctas.	a) Sí, a la Policía b) Sí, a [NOMBRE DEL PROVEEDOR DE SERVICIOS DE INTERNET] (la empresa que le facilita la conexión a Internet) c) Sí, a [NOMBRE DE LÍNEA DIRECTA], un equipo cualificado para recibir y reaccionar a las notificaciones relacionadas con la incidencia de contenidos ilícitos en Internet. d) No, nunca informo, sólo cierro la página	a) – c) Sí, así es. Recuerde que no ha de tener una actitud pasiva cuando encuentre contenidos ilícitos en Internet. Ese tipo de contenidos como pornografía infantil, racismo o xenofobia deberá ser comunicado a la línea directa que opere en su país, a la policía o al proveedor de servicios de Internet. d) Recuerde que lograr el Internet que queremos también depende de usted. No sea indiferente a los contenidos ilícitos que encuentre en la red.

Nº	Pregunta	Respuestas	Comentarios
10	¿Su hijo/a ha encontrado alguna vez contenidos ilícitos o nocivos en Internet?	a) Sí, muchas veces b) Sí, una vez c) No, nunca d) No lo sé	a) y b) Para proteger a su hijo/a del contacto con contenidos ilícitos o nocivos deberá haber instalado software de filtrado en el ordenador. No es una protección ni una garantía total, pero reduce el riesgo de estar expuestos a tales contenidos. c) Perfecto. Si no ha instalado todavía software de filtrado en el ordenador, hágalo. d) Hable con su hijo/a y pregúntele si ha encontrado alguna vez contenidos que le hayan molestado. Si no ha instalado todavía software de filtrado en el ordenador, hágalo.
11	¿Qué debería saber su hijo/a cuando utiliza tecnología de par a par?	a) Es prácticamente imposible que entren virus en el ordenador b) Puede ser ilegal descargar ciertos archivos c) Puede incluir contenidos ilícitos o nocivos d) Compartir archivos es más seguro si tiene un cortafuegos	a) Incorrecto. Lamentablemente, tiene las mismas posibilidades de que su ordenador se infecte con un virus con tecnología de par a par que desde la web o con el correo electrónico. Tenga cuidado cuando descargue contenidos mediante tecnología de par a par y asegúrese siempre de que pasa el archivo por un programa antivirus antes de abrirlo (ejecutarlo). b) Correcto. El material con derechos de autor como música, películas o software descar-

Nº	Pregunta	Respuestas	Comentarios
			gado de Internet normalmente estará protegido de igual modo que el material reproducido en otros medios. En muchos países es ilegal descargar material protegido con derechos de autor. Debería explicarle a su hijo/a que antes de descargar cualquier material que otros hayan colgado en Internet, debería asegurarse de que dispone de permiso de los propietarios de los derechos del material a no ser que existan excepciones o defensas del copyright. c) Correcto. Lamentablemente, la tecnología de par a par también se utiliza para distribuir contenidos ilícitos o nocivos. d) Correcto. Con un cortafuegos instalado en el ordenador, al menos podrá reducir el riesgo de que le entren virus. Un cortafuegos es como un filtro que puede eliminar el *malware* que intenta llegar al ordenador a través de Internet y buscar puntos débiles para introducirse.
12	¿Qué debería hacer si mi hijo/a está siendo víctima de acoso cibernético cuando charla por Internet? Una o más respuestas son correctas.	a) Animar a su hijo/a a no reaccionar al acoso cibernético b) Borrar inmediatamente los mensajes o imágenes recibidas por correo electrónico que molesten a su hijo/a	El acoso cibernético es la forma más reciente de acoso, que tiene lugar a través de Internet o de los teléfonos móviles. a) Correcto. Contestando seguramente no se acaba con el acoso. Al contrario, al hacerlo, los

Nº	Pregunta	Respuestas	Comentarios
		c) Asegurarse de que su hijo/a sólo utiliza salas de charla moderadas d) Animar a su hijo/a a hablar con usted sobre el tema e) Decirle a su hijo/a que deje de enviar mensajes electrónicos y de chatear para evitar el acoso cibernético f) Ponerse en contacto con [INSERTAR PUNTO DE CONTACTO PERTINENTE]	acosadores podrían tener más motivación para continuar. b) Incorrecto. No borre nunca mensajes o imágenes recibidas por correo electrónico. Son pruebas. Guárdelas. c) Correcto. En las salas de charla moderadas, hay un adulto que dirige la conversación entre los participantes. e) Incorrecto. Si lo hace, su hijo/a se verá privado/a de las fantásticas posibilidades que ofrece Internet. f) Correcto. Póngase en contacto con [INSERTAR PUNTO DE CONTACTO PERTINENTE]. Ayudan a niños y jóvenes que reciben amenazas cuando utilizan Internet y teléfonos móviles. **Consejos básicos** • Anime siempre a su hijo/a a hablar con usted si le sucede algo que le molesta o le asusta en Internet. • Controle la actividad en línea de su hijo/a para asegurarse de que no está en contacto con acosadores. • Enseñe a su hijo/a a proteger su privacidad en línea. • Enseñe a su hijo/a a no reaccionar a ningún

Nº	Pregunta	Respuestas	Comentarios
			tipo de acoso como mensajes electrónicos negativos y mensajes de chat agresivos o provocadores. Si su hijo/a sufre acoso cibernético informe de ello a [INSERTAR UNO O MÁS PUNTOS DE CONTACTO PERTINENTES].

Cuestionario para usuarios finales

Cuestionario para usuarios finales

Introducción al perfil del cuestionario para usuarios finales

Le damos la bienvenida al cuestionario de sensibilización ENISA para usuarios finales!

El objetivo de este cuestionario es ofrecerle, como usuario final, una herramienta para comprobar su nivel de sensibilización y su grado de conocimiento de una serie de temas en relación con el uso que hace del ordenador y de los servicios en línea de Internet.

Internet es una herramienta fantástica que ofrece abundante y valiosa información y servicios. Sin embargo, también tiene algunos riesgos que debería conocer.

No pretendemos que estas preguntas sean un test completo para conocer su nivel de sensibilización y grado de conocimiento. El objetivo no es otro que ayudarle a tener una idea de su nivel de sensibilización y, en el mejor de los casos, ofrecerle una herramienta para despertar su interés sobre los valores y los riesgos que comporta el hecho de que utilice Internet. También esperamos que las fuentes de información que se ofrecen en este sitio web le sean de utilidad.

Nº	Pregunta	Respuesta	Comentarios
1	***Archivos adjuntos en correos electrónicos*** Seleccione la respuesta que cree que mejor corresponde a los riesgos que comportan los adjuntos de los mensajes electrónicos. Una o más respuestas pueden ser correctas.	1. Sólo los archivos adjuntos con la extensión .EXE comportan un riesgo real 2. Todos los archivos adjuntos son potencialmente dañinos y pueden contener virus 3. Si conozco el remitente, y me fío de él, siempre puedo abrir el adjunto 4. Puedo abrir adjuntos con seguridad si tengo instalado un cortafuegos en el ordenador 5. Un programa antivirus reducirá el riesgo de infectarse con virus de archivos adjuntos	1. Incorrecto. Hay una gran cantidad y tipos de extensiones que deberían considerarse sospechosas cuando recibe un correo electrónico. No debería abrir archivos adjuntos a no ser que los hubiese pedido o estuviese esperándolos. 2. Correcto. Lamentablemente, es así. Por eso es tan importante que tenga un software antivirus instalado en el ordenador. 3. Incorrecto. Incluso si conoce a la persona que envía el mensaje, y confía en ella, podría enviarle un archivo infectado inconscientemente. 4. Incorrecto. Un cortafuegos no escanea el contenido de los archivos adjuntos en un correo electrónico. 5. Correcto. El software antivirus reduce considerablemente el riesgo de que el ordenador se infecte con virus. A pesar de que no garantiza que el ordenador no esté infectado, se recomienda encarecidamente que instale un programa antivirus.

Nº	Pregunta	Respuesta	Comentarios
2	***Cortafuegos y programas antivirus*** Compruebe lo que sabe sobre cortafuegos y software antivirus.	1. El software antivirus busca virus en sus discos duros y protege su red privada 2. Un cortafuegos protege los recursos de una red privada de usuarios de otras redes 3. El software antivirus no debería usarse nunca con un cortafuegos 4. Un cortafuegos busca virus en sus discos duros y protege los recursos de una red privada de usuarios de otras redes 5. El software antivirus busca virus en sus discos duros	1. Incorrecto. El software antivirus no protege su red privada. Sólo busca virus en su ordenador. 2. Correcto. Un cortafuegos es un sistema entre la red de su ordenador e Internet. Los cortafuegos analizan los datos que entran y salen de la red y rechazan la información de lugares desconocidos y no seguros. 3. Incorrecto. Debería usar ambos: el software antivirus y el cortafuegos 4. Incorrecto. Un cortafuegos no busca virus. 5. Correcto. El software antivirus escanea sus discos duros y le avisa si encuentra virus. Muchos programa antivirus también escanean en busca de programas *adware* y *spyware*.
3	***Actualizaciones de seguridad/parches*** ¿Qué opciones completarían esta oración? «Parchear el ordenador es importante porque . ."	1. hace menos vulnerable el ordenador a los ataques de los virus 2. los parches eliminan virus 3. se reduce el *spam* en el bandeja de entrada 4. soluciona problemas con un programa informático o su información adjunta 5. todo lo anterior	1. Correcto. Al parchear el ordenador se evitan vulnerabilidades en su sistema operativo o aplicaciones haciendo que el ordenador se vuelva menos vulnerable a los ataques de los virus. 2. Incorrecto. Parcheando el ordenador no se eliminan los virus. Para eliminar virus, deberá instalar un programa antivirus. 3. Incorrecto. Un parche simplemente

Nº	Pregunta	Respuesta	Comentarios
			arregla un problema de seguridad en el sistema operativo o en las aplicaciones. No afecta al tipo de información que recibe por correo electrónico. 4. Correcto. Un parche arregla determinados problemas con el código de un programa informático. 5. Incorrecto.
4	***Contraseñas*** ¿Qué debería incluir una contraseña segura?	1. Su nombre 2. Letras en mayúscula y minúscula 3. Su número de teléfono 4. Su matrícula al revés 5. Tanto letras como números siempre que el total tenga cinco caracteres 6. Una combinación de un cierto número de caracteres alfanuméricos	1. Incorrecto. No debería utilizar una palabra relacionada con su identidad personal 2. Correcto. Al utilizar letras en mayúscula y minúscula, el número de combinaciones aumenta y también la dificultad para averiguar su contraseña 3. Incorrecto. No deberá utilizar combinaciones de caracteres relacionados con su identidad personal 4. Incorrecto. No deberá utilizar combinaciones de caracteres relacionados con su identidad personal, aunque estén deletreados al revés. 5. Incorrecto. Una contraseña de sólo cinco caracteres no se considera suficientemente segura, debería ser al menos de siete, pero a ser posible, más. 6. Correcto. Una contraseña segura con-

Nº	Pregunta	Respuesta	Comentarios
			siste en una combinación de letras mayúsculas y minúsculas, caracteres y números.
5	***Compra segura en línea*** ¿Cómo sabe si compra de forma segura en Internet?	1. Conozco la empresa 2. Venden productos de calidad de marcas famosas 3. Hay un *banner* en la parte superior de la página que indica que es un sitio web seguro 4. La URL del sitio web empieza por ‾https://... ‖ 5. Todo lo anterior	1. Correcto. Compre siempre en empresas que conozca y sitios web en los que confíe. 2. Incorrecto. La calidad de los productos ofrecidos no significa que el vendedor sea serio y el sitio seguro. 3. Incorrecto. No debería fiarse nunca sólo de un *banner*. En su lugar, debería intentar verificar la seguridad del sitio web. Por ejemplo, compruebe que la empresa indica una dirección y un número de teléfono. Si tiene dudas sobre la empresa, llame al número de teléfono y haga preguntas para saber si está todo en regla. También puede ponerse en contacto con [INSERTAR EL NOMBRE DE LA ORGANIZACIÓN/ASOCIACIÓN/AUTORIDAD PERTINENTE] para comprobar la legitimidad de la empresa. 4. Correcto. La «s» que aparece detrás de «http» indica que el sitio web está

Nº	Pregunta	Respuesta	Comentarios
			protegido con SSL (Secure Socket Layer), que es un modo de hacer segura la conexión entre usted y el servidor web de la empresa con cifrado. Además, debería buscar un candado cerrado que debería aparecer en la parte inferior de la pantalla. Si el candado está abierto, deberá tener en cuenta que el sitio podría no ser seguro. 5. Incorrecto. Sólo las respuestas 1 y 4 son correctas. **Consejos básicos** • Compre en empresas que conozca. • Asegúrese de que su conexión es siempre segura con SSL. • Lea la política de seguridad y privacidad del sitio web para conocer el tratamiento que la empresa confiere a la información confidencial como números de las tarjetas de crédito y datos personales. • Imprima siempre copias de sus pedidos. • Conozca sus derechos. Las transacciones que realiza en línea

Nº	Pregunta	Respuesta	Comentarios
			están reguladas en virtud de la ley [AÑADIR INFORMACIÓN SOBRE LA LEGISLACIÓN PERTINENTE, REGLAMENTOS ETC. QUE PROTEGEN EL USO DE LAS TARJETAS DE CRÉDITOS EN LAS COMPRAS EN LÍNEA].
6	***Phishing*** Compruebe que conoce los típicos intentos de *phishing* y sabe cómo protegerse de ellos.	1. La información del campo «De» parece ser de la empresa legítima mencionada en el correo electrónico 2. Si uso un programa antivirus estaré protegido contra los intentos de *phishing* 3. Normalmente piden información personal como nombres de usuario, contraseñas y números de la tarjeta de crédito 4. Los correos electrónicos con enlaces/URL a direcciones web son más peligrosos que otros 5. Normalmente el remitente pide que se le responda en un plazo de días 6. Todo lo anterior	1. Correcto. Recuerde: es muy fácil cambiar la información del campo «De» en cualquier cliente por correo electrónico. 2. Incorrecto. Sin embargo, utilizar un programa antivirus reduce el riesgo de infectarse con virus y puede avisar si un mensaje incluye enlaces o adjuntos. 3. Correcto. Recuerde: los bancos y las compañías legítimas nunca le pedirán información personal por correo electrónico ni le pedirán que cambie datos como el nombre de usuario o la contraseña. Si recibe una petición de este tipo, borre inmediatamente el mensaje de su bandeja de entrada y de la papelera de su cliente de correo electrónico para evitar abrirlo involuntariamente. 4. Correcto. No debe hacer clic nunca en

Nº	Pregunta	Respuesta	Comentarios
			un enlace desde el cuerpo del mensaje electrónico. En un intento de *phishing*, el texto del enlace no se corresponde con un sitio web legítimo. Sin embargo, tenga cuidado con cualquier mensaje que le solicite información confidencial. 5. Incorrecto. En la mayoría de los casos, los *phishers* quieren que reaccione de inmediato. Considere estas solicitudes como una advertencia. 6. Incorrecto. Sólo 1, 3 y 4 son correctas. **Consejos básicos:** Comprobando los elementos que se detallan a continuación reducirá el riesgo de ser víctima de un intento de *phishing*. Hágase estas preguntas cuando reciba mensajes sospechosos. **Legitimidad:** ¿La solicitud parece legítima y normal? Por ejemplo, ¿es normal que se solicite esta información y éste es el modo normal de facilitarla? **Importancia**: ¿Cuál es el valor de la información que se le pide o la tarea que se le solicita que realice, y cómo podría

Nº	Pregunta	Respuesta	Comentarios
			emplearse mal? **Fuente**: ¿Tiene la seguridad de que la fuente de la solicitud es auténtica? ¿Tiene modo de comprobarlo? **Plazo de tiempo**: ¿Tiene que contestar en el momento? Si todavía tiene dudas, tómese su tiempo para realizar más comprobaciones o solicitar ayuda. Si recibe un mensaje electrónico que cree que es intento de *phishing*, póngase en contacto con: [INSERTAR NOMBRE DE AUTORIDAD/ASOCIACIÓN/ORGANIZACIÓN PERTINENTE].
7	***Copia de seguridad*** Compruebe lo que sabe sobre las copias de seguridad de los datos.	1. Sólo debería realizar copias de seguridad de las fotos que tenga en el ordenador 2. Debería realizar una copia de seguridad de cualquier información que considere importante 3. De los archivos que no se vayan a modificar en el futuro sólo hay que hacer una copia de seguridad 4. No debería utilizar nunca un CD-RW como unidad de almacenamiento externo 5. Debería tener los archivos copiados en el mismo lugar en donde tiene los archivos originales por si los necesita en algún momento	2. Incorrecto. Debería hacer copias de seguridad de cualquier archivo que sea importante para usted. 3. Correcto. Por ejemplo: • Fotos • Software o música que haya comprado y descargado de Internet • Agenda de correo electrónico • Cartas y mensajes electrónicos 4. Correcto. Sin embargo, cuantas más copias de seguridad tenga, mejor. 5. Incorrecto. Los CD-RW son unidades de almacenamiento excelentes. Pue-

Nº	Pregunta	Respuesta	Comentarios
			den almacenar cantidades relativamente importantes de datos y son bastante económicos. Hay además otras unidades de almacenamiento, cada una con sus ventajas y desventajas, por ejemplo: • Discos externos • Memorias USB • Almacenamiento y copias de seguridad en línea 6. Incorrecto. Siempre es mejor guardar las copias de seguridad en un lugar diferente del ordenador. En el mejor de los casos debería tener varias copias de seguridad guardadas en diferentes sitios. Si guarda documentos importantes en una caja fuerte del banco, por ejemplo, también debería guardar una copia de seguridad de sus archivos.
8	***Memorias USB*** Las memorias USB son una unidad de almacenamiento de datos cada vez más utilizada. Pero, ¿es consciente de los riegos y las desventajas de las memorias USB?	1. No pueden guardar fotos 2. Pueden tener virus 3. Son caras en relación con la capacidad de almacenamiento que tienen 4. Son fáciles de perder 5. Son un modo seguro de almacenar datos porque las memorias USB están cifradas	1. Incorrecto. Puede guardar cualquier tipo de archivos en una memoria USB al igual que en cualquier otra unidad de disco. Esa es una de las ventajas de las memorias USB. 2. Correcto. Antes de utilizar una memoria USB debería escanearla para com-

Nº	Pregunta	Respuesta	Comentarios
			probar si tiene virus. Debería hacerlo además cada vez que copie archivos de un ordenador en el que no confía. 3. Incorrecto. Una de las principales ventajas de las memorias USB es su precio relativamente reducido si tenemos en cuenta su alta capacidad de almacenamiento. 4. Correcto. El hecho de que sean pequeñas a veces es una ventaja, pero inevitablemente son más fáciles de perder. 5. Incorrecto. Normalmente, las memorias USB no traen ninguna función de cifrado. A fin de proteger los datos, debería cifrar los archivos almacenados en las memorias USB utilizando hardware o software de cifrado. Si la perdiese, nadie podría acceder a los datos. Si además tiene una copia de seguridad de esos archivos, no tendrá ningún problema aunque la pierda.
9	***Cifrado*** Cifrar es un modo de proteger información, pero ¿cuánto sabe sobre el cifrado?	1. El cifrado resulta caro para algunos usuarios particulares 2. Normalmente, los archivos que están cifrados no se pueden revelar a otros 3. No todos los datos se pueden cifrar 4. Los mensajes electrónicos no tienen que es-	1. Incorrecto. El software de cifrado no tiene por qué ser caro. Hay incluso *freeware* de cifrado. Cuando elija el programa de cifrado, asegúrese de que el código fuente es de uso público. Esto permite a los expertos en

Nº	Pregunta	Respuesta	Comentarios
		tar cifrados a no ser que se envíen con adjuntos 5. El cifrado protege la confidencialidad de la información	programación y cifrado examinarlo y buscar «puertas traseras» y errores. 2. Correcto. El software de cifrado de archivos más conocido consiste en utilizar algoritmos muy seguros que son prácticamente imposibles de descifrar. 3. Incorrecto. Todos los datos se pueden cifrar. Sin embargo, algunos programas de cifrado sólo sirven para cifrar mensajes electrónicos, mientras que otros también ofrecen cifrado de archivos e incluso del disco duro. 4. Incorrecto. Podrá cifrar cualquier dato que desee cifrar. 5. Correcto. El cifrado es un modo de evitar revelar información sin autorización.
10	***Descargar archivos*** Internet es un recurso fantástico que ofrece toda su información con sólo un clic. Pero, ¿conoce los aspectos relativos a los derechos de autor de los archivos que se descargan?	1. Es ilegal descargar material protegido con derechos de autor publicado ilegalmente 2. Es ilegal descargar cualquier material protegido por derechos de autor 3. Es legal descargar música siempre y cuando no sea en formato MP3 4. Es ilegal colgar/compartir material protegido por derechos de autor publicado ilegalmente 5. El software no es material protegido por de-	[LAS RESPUESTAS A ESTA PREGUNTA DEBERÁN AÑADIRSE Y MODIFICARSE PARA CUMPLIR LA LEGISLACIÓN APLICABLE EN SU PAÍS]. 1. 2. 3. 4. 5.

Nº	Pregunta	Respuesta	Comentarios
		rechos de autor, sólo los textos, la música, las fotos y las películas	

Cuestionario para PYME

Introducción al cuestionario para PYME

Cuestionario para PYME

Le damos la bienvenida al cuestionario de sensibilización ENISA para directivos de PYME!

El objetivo de este cuestionario es ofrecerle, como directivo de una empresa mediana o pequeña, una herramienta para comprobar su nivel de sensibilización y grado de conocimiento sobre una serie de temas en relación con el uso que hace de los ordenadores e Internet como herramienta de asistencia a su actividad empresarial. Estas herramientas son muy valiosas para aumentar la capacidad que tiene su empresa para comunicarse y competir en un mercado europeo y mundial. Sin embargo, también comportan riesgos que debería conocer.

No pretendemos que este cuestionario sea un test completo para conocer su nivel de sensibilización y grado de conocimiento. El objetivo no es otro que ayudarle a tener una idea de su nivel de sensibilización y, en el mejor de los casos, ofrecerle una herramienta para despertar su interés sobre los valores y los riesgos que comporta el hecho de que utilice Internet. También esperamos que las fuentes de información que se ofrecen en este sitio web le sean de utilidad.

Perfil de riesgo

La gestión de la seguridad de las redes y de la información es básicamente una actividad de gestión del riesgo, y como tal, un requisito para identificar los activos de valor para las empresas dañados por la existencia de puntos débiles en los sistemas de TI. Además de los procesos de producción, la información es un activo valioso que a menudo está en riesgo debido a fallos de los sistemas de TI.

Entre la información valiosa cabe destacar, por ejemplo, bases de datos de información de proveedores y agendas de clientes (también en equipos portátiles), información económica, modelos industriales y planes de empresa. La información es un activo y como tal, está en riesgo por muchas amenazas como peligros naturales, delitos, fallos del sistema y errores humanos.

Nº	Pregunta	Respuestas	Comentarios
1	¿Sabe qué información importante se procesa en sus sistemas de TI y dónde?	a) Sí, tenemos un inventario detallado de información importante que utilizamos, por ejemplo, para copias de seguridad b) Sí, sabemos que algunos sistemas son muy importantes porque procesan información muy valiosa c) No, sabemos que hay información valiosa en nuestros sistemas, pero no sabemos exactamente cuál y dónde d) No, no tenemos información realmente muy valiosa en nuestros sistemas e) No lo sé	Conocer bien qué información importante se procesa en los sistemas de TI es la base para una gestión adecuada de los riesgos. Este conocimiento es fundamental para aplicar controles adecuados (por ejemplo, mecanismos de protección) y realizar inversiones eficaces. Conozca a su enemigo. Es la forma de invertir en las mejores contramedidas.

Nº	Pregunta	Respuestas	Comentarios
2	¿Cuál de las siguientes amenazas es la más peligrosa para la información de su empresa?	a) Los competidores, porque la competencia es muy fuerte en este mercado b) Los socios, porque tenemos que compartir la información valiosa con muchos agentes c) Los delincuentes, porque mi empresa desarrolla actividades comerciales para particulares d) Los empleados, porque podrían filtrar información intencionada o no intencionadamente e) Ninguna f) No lo sé	

Aspectos legales y contractuales

Los directivos tienen que atenerse a la ley y cumplir las obligaciones legales. En el ámbito de la seguridad de las redes y la información, hay que tener en consideración varias leyes europeas y/o nacionales y aplicarlas a las actividades de la empresa. ¿Conoce sus responsabilidades legales en relación con la seguridad de la información?

Nº	Pregunta	Respuestas	Comentarios
3	¿Conoce la regulación sobre privacidad aplicable en su país/Europa (en relación con los datos de sus clientes)? ¿Es consciente del impacto en la gestión de TI?	a) Sí, este proceso está bajo control b) No, no nos ocupamos de estas cuestiones legales c) En parte, hemos puesto en marcha recientemente un proceso de mejora d) No lo sé	El cumplimiento de cuestiones legales sobre la seguridad de las redes y de la información tiene cada vez más importancia. Los directivos deben ser conscientes de sus responsabilidades legales. La protección de los datos personales y la

Nº	Pregunta	Respuestas	Comentarios
4	¿Conoce la regulación sobre derechos de autor aplicable en su país/Europa (en relación con el software y los contenidos digitales)?	a) Sí, este proceso está bajo control b) No, no nos ocupamos de estas cuestiones legales c) En parte, hemos puesto en marcha recientemente un proceso de mejora d) No lo sé	gestión de licencias de software son muy importantes en este ámbito. En caso de subcontratar, las obligaciones de los contratistas deberían estar claramente especificadas en los contratos. Esto incluye manejar datos confidenciales en sistemas de información durante las actividades de mantenimiento.
5	¿Ha implementado obligaciones contractuales para proteger la seguridad de las redes y de la información cuando sus sistemas se subcontraten, por ejemplo, para mantenimiento?	a) Sí, este proceso está bajo control b) No, no subcontratamos c) En parte, hemos puesto en marcha recientemente un proceso de mejora d) No lo sé	

Aspectos organizativos y humanos

Las herramientas de seguridad son muy útiles para proteger las redes y los sistemas de información. Sin embargo, al igual que sucede con la seguridad en la conducción, sólo el comportamiento de los conductores puede reducir seriamente los accidentes. Sus empleados deberían tener conocimientos básicos y saber cómo manejar la información y los ordenadores.

¿Cómo se reflejan en la política de seguridad de la información (explícita o implícita) de su empresa las siguientes cuestiones?

Nº	Pregunta	Respuestas	Comentarios
6	¿Quién conoce la contraseña que se utiliza para acceder a los datos de su empresa?	a) Sólo usted b) Sólo unos cuantos colegas c) Sólo un administrador del sistema d) Miembros de la familia	Una serie de actitudes básicas y estar alerta ante ciertas situaciones de riesgo puede reducir considerablemente los riegos de la seguridad de la información. Los directivos tienen un papel importante en la creación de una cultura de la seguridad de la información ya que tienen que dar buen ejemplo. Internet es un entorno nuevo, como un país extranjero: es necesario adoptar la actitud adecuada para evitar el fraude y los riesgos. Empiece por definir la política de seguridad. Encontrará más información aquí: [INTRODUCIR MÁS INFORMACIÓN Y/O IN-
7	¿Utiliza su dirección electrónica privada en su actividad profesional?	a) Nunca b) A veces c) Con frecuencia d) Todos los días	
8	¿Trata cuestiones profesionales en plataformas de comunicación o grupos de noticias?	a) Nunca b) A veces c) Con frecuencia d) Todos los días	
9	¿Contestaría a una llamada de teléfono o un mensaje electrónico en el que se le solicita información sobre la empresa?	a) Yo nunca contesto b) Contesto las preguntas c) Pido detalles antes de contestar d) Pido consejo a un compañero o a un amigo e) No lo sé	

Nº	Pregunta	Respuestas	Comentarios
10	¿Están sus dispositivos portátiles (PDA, ordenadores portátiles, memorias USB) siempre bajo control y vigilancia cuando no se están utilizando?	a) Sí b) No c) A veces d) No tengo ningún dispositivo de ese tipo e) No lo sé	SERTAR ENLACES DONDE SE PUEDA ENCONTRAR MÁS INFORMACIÓN]

Herramientas de seguridad

Una vez identificados los activos de información, hay varias técnicas básicas para protegerlos de manera eficaz. Los virus, los ataques de *spyware*, la intrusión en la red o la revelación/robo de información pueden tener un efecto importante en las actividades empresariales.

¿Conoce las herramientas de seguridad destinadas a proteger los dispositivos y la información confidencial?

Nº	Pregunta	Respuestas	Comentarios
11	Se realizan copias de seguridad de los datos confidenciales:	a) Diariamente b) Semanalmente c) Mensualmente d) Nunca e) No lo sé	Algunas soluciones básicas son suficientes para proteger los sistemas de información de las empresas. Los que se citan en las preguntas son ahora fáciles de usar y rentables. No utilizarlos incrementará considerablemente la exposición al riesgo y la posibilidad de que el sistema se dañe por cuestiones triviales.
12	Se han instalado y actualizado programas antivirus y *antispyware*:	a) En PC b) En ordenadores portátiles c) En servidores de archivos d) En servidores de correo electrónico e) No lo sé	

Nº	Pregunta	Respuestas	Comentarios
13	Se han instalado soluciones de acceso remoto seguro en PDA y ordenadores portátiles (con VPN y autenticación segura)	a) Sí b) No c) En progreso d) No lo sé	
14	El cifrado se utiliza para cifrar:	a) Datos en PC b) Datos en ordenadores portátiles, PDA y otros dispositivos portátiles c) Datos en servidores de archivos d) Correos electrónicos e) No lo sé	

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu