GOBIERNO DE ARAGON

Guía para el profesor del taller

“SEGURIDAD EN INTERNET”

Presentación. Taller de “Seguridad en internet”

Desde el Departamento de Ciencia, Universidad y Sociedad del Conocimiento, se promueve la realización de este taller, con el objetivo de acercar a los participantes al mundo TIC, enseñando a utilizar de forma segura y adecuada las gestiones que los participantes necesiten.

Este manual forma parte de los materiales de la formación presencial que se lleva a cabo en centros públicos o de uso público de diversas localidades de la Comunidad Autónoma de Aragón.

Parte del contenido del presente taller se ha basado en el Manual de experiencia senior en ciberseguridad[1] desarrollado por la empresa INICIBE[2] y la oficina de seguridad del internauta[3].

Realización de este manual: noviembre de 2022.

Talleres TIC [4]

Talleres TIC. Manuales; 23

GOBIERNO DE ARAGON

[1] https://www.osi.es/sites/default/files/docs/senior/guia_ciberseguridad_para_todos.pdf
[2] https://www.incibe.es/
[3] https://www.osi.es/es
[4] https://www.aragon.es/-/talleres-tic

Índice de contenidos

01. Presentación de la guía didáctica al profesor

Este curso básico tiene como objetivo dar a conocer los riesgos que puede haber en internet y cómo defenderse de los mismos, a personas que tienen unos conocimientos limitados al respecto.

Esta guía para el docente del curso se presenta con el objeto de facilitar la función del aprendizaje del alumno, presenta los conceptos básicos sobre seguridad en internet y ofrece a los alumnos la posibilidad de comprobar la protección de sus dispositivos y configurar la seguridad de los mismos.

Los medios e infraestructura necesarios para el seguimiento del taller están formados por una sala equipada con ordenadores conectados a Internet y un proyector de pantalla, para que los alumnos puedan seguir los pasos en el monitor del profesor.

Se recomienda que cada alumno disponga de sus propios dispositivos móviles o tabletas, aunque se puede realizar por parejas, en caso de que el número de dispositivos sea insuficiente.

02. Objetivos generales

Los objetivos generales del curso son los siguientes:

- Entender que existen riesgos al utilizar internet.
- Aprender a identificar y conocer los posibles fraudes en la red.
- Aprender a mantener los equipos y programas actualizados.
- Saber cómo actuar en caso de un fallo de seguridad.

03. Temporalización

La duración prevista de este curso básico es de 5 horas.

Se recomienda atenerse a dicha duración, teniendo en cuenta el carácter de los contenidos de este curso. Para facilitar la asimilación de los pasos y conceptos se ha dividido el contenido en dos bloques diferenciados, cada uno con actividades para favorecer una perspectiva experimental en el aprendizaje, estas actividades se intercalarán con la teoría.

De esta forma, la estructura temporal estaría formada así:

• Exposición teórica: 1 hora.

• Parte práctica: 4 horas

04. Metodología

La metodología propuesta para este curso ha de ser eminentemente práctica, favoreciendo un papel activo y autónomo por parte del alumno, y en la que el profesor ha de ser, ante todo, un facilitador del proceso de enseñanza-aprendizaje.

De esta forma, el profesor debe procurar que las exposiciones teóricas no sean muy extensas e incluso realizarlas a la vez que los alumnos siguen los pasos de manera práctica.

Será muy positivo que desde el inicio el alumno conecte con sus motivaciones para realizar este curso, para ir avanzando en los aspectos prácticos de uso de las plataformas presentadas.

El profesor alternará el trabajo individual del alumno y fomentará su autonomía con el trabajo en un grupo pequeño (por parejas, por ejemplo), impulsando así el aprendizaje colaborativo mediante la cooperación.

La metodología desarrollada debe permitir, además, que el alumno pueda comprobar el avance en su propio proceso de aprendizaje, por lo que las actividades deben poseer carácter formativo a través del logro de los objetivos generales planteados.

05. Propuesta de contenidos y actividades

5.1. ¿Qué es la seguridad informática?

Introducción

El inicio de este curso debe comenzar con una dinámica para que el profesor conozca a sus alumnos y sus motivaciones, creando de esta manera un clima de confianza.

Es importante explicar los objetivos que esperamos que alcancen los alumnos de este curso y la metodología que vamos a utilizar, animando a la participación y a que el alumno asuma un papel activo y protagonista.

ACTIVIDAD: Sin perder de vista nuestro objetivo, aprovecharemos para que nuestros alumnos se presenten y expliquen qué esperan conseguir con este curso, para conectar con sus motivaciones y facilitar nuestra adaptación a sus expectativas e intereses, así como a sus características personales.

¿Qué es la seguridad informática?

En este apartado realizaremos una breve introducción en la que se explican los conceptos básicos sobre la seguridad informática:

- ¿Qué es un sistema operativo?
- ¿Qué es un virus informático?
- ¿Para qué sirven los antivirus?
- ¿Nos pueden engañar por internet?

Las explicaciones pueden variar dependiendo de los conocimientos previos que posean los alumnos.

ACTIVIDAD: Será importante implicar a los alumnos, preguntándoles directamente por sus conocimientos previos.

Se aclararán los conceptos de:

- Ciberseguridad
- Seguridad informática
- Seguridad de la información
- Malware

¿Por qué es necesario protegerse?

Plantearemos a los alumnos esta pregunta e intentaremos relacionarla con el uso que hacen de internet en su día a día. Después y paso a paso se les mostrará cómo comprobar si se encuentran protegidos en cada uno de sus dispositivos.

Los alumnos pueden seguir al profesor que mostrará en el proyector, el proceso paso por paso o seguir los pasos recogidos en el manual para los dispositivos:

- Windows 10
- Android
- MacOS
- iOS

5.2. ¿Cuáles son los riesgos más comunes?

En esta parte del curso veremos los riesgos más comunes que se pueden sufrir y se preparará a los alumnos para la siguiente parte del curso en la que se les enseñará cómo evitar estos riesgos.

En la medida de lo posible procuraremos que integre un contenido práctico, aunque la parte más práctica se encuentra en la siguiente sección.

A la hora de llevar a cabo partes más prácticas utilizaremos como referencia el manual del curso para que los alumnos sigan paso a paso cada proceso. Idealmente cada alumno utilizará su propio dispositivo de manera individual, en caso de no haber suficientes dispositivos pueden trabajar por parejas. El profesor utilizará un ordenador y un proyector para guiar a los alumnos en su proceso.

Fraudes y engaños

Para iniciar esta parte se enumerará a los alumnos los diferentes tipos de fraudes y engaños a los que se pueden enfrentar:

- Falsos chollos
- Métodos de pago
- Otros tipos de fraudes y engaños

ACTIVIDAD: Se iniciará un diálogo con los alumnos para que aporten sus ideas sobre cómo identificar estos fraudes o engaños.

Una vez se han recogido sus sugerencias se procede a explicar uno por uno cómo se podrían evitar o localizar.

Ingeniería social

A continuación, el docente explicará los ataques de ingeniería social en los que mostrará los diferentes tipos, además de sus diferencias y objetivos. Se aclararán los diferentes tipos:

- Pishing
- Vishing
- Smishing
- Spam

ACTIVIDAD 1: Los alumnos podrán aportar sus experiencias con cualquier tipo de correo electrónico o número de teléfono no habitual que hayan tenido.

ACTIVIDAD 2: A partir de las experiencias que han tenido, entre todos intentarán elaborar una lista de acciones que podrían haber llevado a cabo para detectar estas comunicaciones fraudulentas. El docente utilizará esta información para profundizar en los pasos a seguir para la identificación de este tipo de ataques.

Noticias falsas

Se explicará cómo las noticias falsas cada vez tienen medios de difusión más amplios.

ACTIVIDAD: Se iniciará un diálogo con los alumnos para que aporten sus experiencias con noticias falsas.

Aprovecharemos las respuestas para aclarar conceptos e introducir los métodos de identificación.

Se terminará con los consejos para identificar noticias falsas poniendo especial énfasis en la necesidad de contrastar las noticias con varias fuentes para comprobar su veracidad.

Tipos de amenazas

Para terminar este primer bloque se explicará a los alumnos que aparte de todo lo anterior pueden sufrir ataques directos por parte de terceros. Estos ataques pueden ser:

- Ataques a contraseñas
- Ataques por Malware

5.3. Actividad 1

Este apartado al ser eminentemente práctico, pretende que los alumnos se involucren de forma activa en su propia ciberseguridad.

Identificar las amenazas

Se animará a los alumnos para que creen una lista sobre las actividades diarias para las que utilizan internet y se les pedirá que las relacionen con amenazas que se hayan visto en esta sesión.

Además, se les animará a que comprueben si sus dispositivos están protegidos.

Tests de ciberseguridad

Como ejercicio opcional se propondrá a los alumnos realizar el Test de ciberseguridad[5] y el Test de compras por internet[6].

[5] https://www.osi.es/es/test-evaluacion/ponte-prueba-cuanto-sabes-sobre-ciberseguridad
[6] https://www.osi.es/es/test-evaluacion/ponte-prueba-viii-cuanto-sabes-sobre-ciberseguridad

5.4. Mecanismos de seguridad

Este apartado va a permitir a los alumnos experimentar y conocer paso por paso cómo llevar a cabo cada una de las funciones que se ha nombrado en los apartados anteriores.

Cómo en ocasiones anteriores utilizaremos como referencia el manual del curso para que los alumnos sigan paso a paso cada proceso. Idealmente cada alumno utilizará su propio dispositivo móvil de manera individual, en caso de no haber suficientes dispositivos pueden trabajar por parejas. El profesor utilizará un ordenador y un proyector para guiar a los alumnos en su proceso.

¿Cómo proteger nuestra privacidad y nuestros datos?

Se explicará el funcionamiento de los métodos de protección como:

- Contraseñas
- Verificación en dos pasos
- Diferentes bloqueos de dispositivos

Y se darán consejos para establecer contraseñas robustas y hacer que nuestros sistemas de protección sean lo más efectivos posibles.

Uso de antivirus para tu Smartphone

En este apartado se explican los conceptos de antivirus, profundizando en los tipos de antivirus y se explica la existencia de tres antivirus gratuitos.

- Google protect
- AVG
- Kaspersky

Además de cómo descargarlos y las características de cada uno.

ACTIVIDAD: Se iniciará un diálogo con los alumnos para que cuenten si saben qué antivirus tienen o si alguna vez han perdido información a causa de algún virus.

Alertas y consejos

Se terminará el curso dando a los alumnos una serie de consejos y advertencias a los que deben estar atentos a la hora de usar internet:

- Consejos: Descarga segura de aplicaciones
- Consejos: Mantén tu sistema operativo y antivirus actualizados
- Consejos: Realiza copias de seguridad
- Alerta: E-mails extraños

5.5. Actividad 2

Este apartado, al ser eminentemente práctico, pretende que los alumnos conozcan de primera mano el funcionamiento del sistema de actualización de su antivirus y su sistema operativo.

Sistema operativo

Se guiará a los alumnos, para que actualicen el sistema operativo de su Smartphone.

Antivirus

Se les animará a comprobar que el antivirus está activado y en caso de no estarlo se instalarán un antivirus.

5.6. Evaluación

Este último capítulo propone una última actividad dividida en dos partes, cada una de ellas se le estima una duración de 15 minutos.

Reflexión

En esta ronda de reflexión los participantes en el curso, compartirán su opinión y plantearán las dudas que tengan, el educador recogerá las preguntas y se intentarán resolver en la siguiente parte.

Ronda de dudas

Las dudas, comentarios o sugerencias sobre el curso, la aplicación o la página web se habrán recogido por el educador y entre todos intentarán resolverlas. En caso de no poder resolver alguna de las dudas se les enviará una respuesta por email a los participantes.

ACTIVIDAD: Se propone que los alumnos realicen los tests de ciberriesgos y compras por internet (enlaces en los anexos) para evaluar su experiencia tras el curso.

06. Anexos

6.1. Enlaces y referencias

Páginas Webs importantes:

- Sellos de confianza online[7]
- Oficina de seguridad del internauta[8].
- Test de ciberseguridad[9]
- Test de compras por internet[10]
- Instituto nacional de ciberseguridad[11]
- Política de Google de Software No Deseado[12]
- Manual de experiencia senior en ciberseguridad[13]
- Google drive[14]
- Dropbox[15]
- OneDrive[16]

[7] https://protecciondatos-lopd.com/empresas/sellos-de-confianza-online/
[8] https://www.saludinforma.es/portalsi/web/salud/tramites-gestiones/cita-previa
[9] https://www.osi.es/es/test-evaluacion/ponte-prueba-cuanto-sabes-sobre-ciberseguridad
[10] https://www.osi.es/es/test-evaluacion/ponte-prueba-viii-cuanto-sabes-sobre-ciberseguridad
[11] https://www.incibe.es/
[12] https://www.google.com/about/unwanted-software-policy.html
[13] https://www.osi.es/sites/default/files/docs/senior/guia_ciberseguridad_para_todos.pdf
[14] https://drive.google.com/
[15] https://www.dropbox.com/
[16] https://onedrive.live.com/