Centro de Estudios de Postgrado

Máster en Profesorado de Educación Secundaria Obligatoria y Bachillerato, Formación Profesional y Enseñanza de Idiomas

UNIVERSIDAD DE JAÉN

Centro de Estudios de Postgrado

Trabajo Fin de Máster

TIPOS DE ATAQUES Y SOFTWARE MALICIOSO. HERRAMIENTAS PREVENTIVAS Y PALIATIVAS. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Alumno/a: **López Expósito, José**

Tutor/a: Prof. D. Francisco R. Feito Higueruela y Rafael Segura Sánchez

Dpto: Informática

Junio, 2015

Table of Contents

1.1 Resumen

En este trabajo se presenta un proyecto para llevar a cabo en la asignatura de informática de 4º de ESO del IES Virgen del Carmen de Jaén, para desarrollar el tema "tipos de ataques y software malicioso, herramientas preventivas y paliativas". Se ha elegido una metodología basada en proyecto. Se pretende que mediante un juego de roles que proponga situaciones reales de la vida, el alumnado sea capaz de desenvolverse y de entender la magnitud y la importancia del tema. Además permitirá que se implique en la investigación del mismo y le facilitará el aprendizaje de los aspectos a trabajar, ayudando a entender las consecuencias que tienen sobre la vida de los demás los actos que cometen. Es una metodología muy innovadora y que plantea un reto importante para el profesor, pero se espera un resultado muy positivo tanto para el profesor como para el alumnado.

1.2. Palabras clave

Metodología basada en proyecto, ética informática, seguridad informática, ataques informáticos, herramientas paliativas, herramientas preventivas, malware.

1.3. Abstract

In this work I propose a project to be developed for the computer course that takes place in the 4th year of ESO in the IES Virgen del Carmen in the city of Jaén. The subject-matter that we will be dealing with is called "types of hacking and malware, antimalware and backup tools". A project-oriented methodology has been chosen in its development. Across this project it is intended a roleplay to be done, proposing real life situations, so that the student is able to understand the magnitude of the subject. It will also give them the ability to research the matter to ease his learning, understanding the impact of their actions on the life of others. It is a very innovative methodology which raises a big challenge for the teacher, but it is expected to have a very positive result, not only for the students but also for the teacher.

1.4. Key words

Project-oriented methodology, computer ethics, hacking, backup tools, antimalware, malware.

2. Introducción

Este trabajo ha sido llevado a cabo tras la realización del practicum del Master de Educación Secundaria, que tuvo lugar en el IES Virgen del Carmen de la ciudad de Jaén. Durante ese practicum se pusieron en práctica las metodologías y las estrategias aprendidas en el máster. Fue una forma de entrar en contacto con la docencia y poner en práctica metodologías innovadoras.

El tema a trabajar son los tipos de ataques informáticos y de malware que hay y las formas de prevenirlos y de reponerse ante uno.

La intención de la unidad didáctica desarrollada es la de alimentar en el alumnado el espíritu crítico que le permita conocer las consecuencias de los malos actos que podemos desarrollar a través de Internet para conocer el alcance y la importancia del mismo.

Se ha desarrollado una metodología basada en proyecto, un método innovador fundamentado en la creación de una especie de juego de roles que permita meterse en papeles que simulan situaciones de la vida real. Esta metodología fomenta la implicación y el interés del alumnado en el tema, y proporciona una empatía con los demás alumnos y alumnas.

3. Fundamentación epistemológica

3.1. Contextualización del centro escolar

Como viene recogido en el Plan de Centro del IES Virgen del Carmen [1], el centro se encuentra situado en la zona céntrica de la ciudad de Jaén, con buena comunicación ubicado en la intersección de dos de las vías de comunicación principales de la localidad, lo que propicia que, en buena medida, el alumnado que solicita este Instituto en los niveles de ESO y Bachillerato, no tenga su domicilio familiar en la zona, y sea por tanto, el domicilio de trabajo de alguno de sus progenitores el aportado a la hora de la solicitud de matriculación. En lo que al alumnado de Formación Profesional respecta, el abanico de posibilidades se abre, ya que existen Ciclos Formativos que tienen un ámbito provincial; no obstante por la ubicación del centro, próximo a la Estación de Autobuses, es un factor que no supone una carga añadida para que el alumnado pueda cumplir con su horario de permanencia en el Instituto.

En general, las familias del alumnado del centro se dedican, fundamentalmente, al sector servicios, pudiendo ser clasificadas dentro de un estrato medio de la población en cuanto a su nivel de ingresos. Pertenecen, generalmente, a familias estructuradas

donde la mayoría de los miembros cohabitan en el núcleo familiar, disponiendo de los espacios básicos para poder realizar sus actividades de estudio y de ocio.

Un grupo de alumnos, menor que el anterior, tiene familias dedicadas al sector primario pero, en general, las características familiares son similares a las expuestas anteriormente.

Por último, podemos encontrar un tercer grupo de alumnado procedente de otros países, y que se integran en el Instituto con un nivel académico inferior a la media, y sobre el cual hay que realizar medidas de apoyo educativo para facilitar su integración personal y escolar.

En la generalidad del centro, el nivel de estudios de los padres es medio. En una buena parte de los domicilios existe ordenador y acceso a libros que pueden ser utilizados por el alumnado.

Las aficiones fundamentales del alumnado son el deporte, salir con los amigos, ver la televisión, jugar con videojuegos y actividades derivadas del uso del ordenador.

El edificio del centro dispone además de las instalaciones destinadas a la docencia tradicional, de otras tales como Biblioteca, Departamentos Didácticos, Laboratorios, Gimnasio, aulas especificas de informática, tecnología, música y plástica, Salón de Actos y distintas dependencias destinadas a despachos y administración. También existen tres pistas deportivas de distinto tamaño que, fuera del horario lectivo, se encuentran disponibles para su utilización por los miembros de la Comunidad Escolar y por asociaciones y colectivos de la zona en la que se encuentra ubicado el Instituto. Estas instalaciones, aunque escasas para el numero de alumnos existentes en el centro, permiten que cada grupo de alumnos tenga asignada su propia aula saliendo solamente de las mismas para realizar actividades específicas. Este extremo influye positivamente en el orden general de centro. No obstante, la reestructuración progresiva de espacios, como consecuencia de la implantación del nuevo sistema educativo, ha repercutido negativamente en la convivencia.

Aparte del material disponible en cada departamento, existe, a disposición del profesorado, material audiovisual e informático:

- En cada una de las plantas del centro hay uno o dos carritos con ordenadores portátiles para uso en las aulas y que están guardados en pequeños recintos cerrados con llave.
- Para la visualización de CD/DVD, hay a disposición del profesorado dos proyectores portátiles para poder trasladarlos a la clase. Con este fin puede usarse también el Salón de Actos del Instituto.
- El centro pondrá a disposición, durante el primer trimestre del curso, para el profesorado que aún no la tenga, una PDA que se utilizará para la gestión de faltas

del alumnado y que podrá usarse también como cuaderno del profesor a través del programa evalúa.

Existe una página web del centro accesible a través del dominio www.iesvirgendelcarmen.com. En ella hay información de interés para el alumnado y para el profesorado, como es el calendario del curso, los documentos, elaborados por el centro, de evaluación de la ESO y del Bachillerato, el ROF del centro, los libros de texto de los alumnos, que están asimismo publicados en los tablones de anuncios del centro, y otra información de interés general.

3.2. Contextualización de la materia: Informática de 4º de ESO

Según la LOE, y en particular de acuerdo a lo establecido en el REAL DECRETO 1631/2006, de 29 de diciembre, por el que se establecen las enseñanzas mínimas correspondientes a la Educación Secundaria Obligatoria [2]:

La sociedad actual se encuentra en un profundo proceso de transformación caracterizado por la presencia de las tecnologías de la información y de la comunicación en una parte importante de la vida cotidiana de las personas, que permiten la posibilidad de expandir la comunicación y generan una cultura que da acceso al desarrollo de nuevas destrezas y formas de construcción de conocimiento y que se encuentra en constante evolución.

Surge así la necesidad de educar en el uso de las tecnologías de la información durante la educación obligatoria y que abarca dos vertientes.

- Los jóvenes deberán adquirir los conocimientos básicos sobre las herramientas que facilitan su interacción con el entorno, así como los límites morales y legales que implica su utilización.
- Deberán ser capaces de integrar los aprendizajes tecnológicos con los aprendizajes adquiridos en otras áreas del currículo, dándoles coherencia y mejorando la calidad de los mismos.

La informática puede ser entendida como el uso y aprovechamiento de las tecnologías de la información y la comunicación en cualquiera de las formas en que éstas se nos presentan. Se trata, no sólo de preparar a los alumnos para desenvolverse en un marco cambiante donde las herramientas de hoy quedarán previsiblemente obsoletas en un corto plazo, además hay que propiciar la adquisición de conocimientos, destrezas y aptitudes que permitan al alumnado continuar con el aprendizaje a lo largo de su vida adaptándose a las demandas que aparecen en su vida. En este contexto, Se

complementan de manera instrumental las aplicaciones informáticas en las diferentes materias curriculares de la Educación Secundaria, y en el cuarto curso, aquéllos que lo deseen, puedan cursar con carácter opcional una materia concreta que venga a complementar los conocimientos técnicos adquiridos previamente.

Los contenidos de la materia se estructuran en cuatro grandes bloques: un primer bloque, dedicado a los sistemas operativos y la seguridad informática, un segundo bloque que abarca las herramientas multimedia, tratamiento de imagen, vídeo y sonido a partir de diferentes fuentes, un tercero que se aproxima a la publicación y difusión de contenidos en la Web, y un último bloque que profundiza en Internet y las redes sociales virtuales, los tipos de «software» y sus licencias y el acceso a los servicios electrónicos. Esta clasificación no debe entenderse como elementos separados. En este sentido cabe señalar la necesidad de formar a los jóvenes en una actitud crítica ante el uso de las herramientas informáticas, para que distingan en qué nos ayudan y en qué nos limitan y poder, así, obrar en consecuencia.

3.3. Contextualización del tema

El tema elegido para el desarrollo de este trabajo es "Tipos de ataques y software malicioso. Herramientas preventivas y paliativas. Sistemas de gestión de la seguridad de la información". En el currículo que establece la LOE para la asignatura de Informática podemos encontrar un primer bloque llamado "Sistemas Operativos y Seguridad Informática" cuyo contenido es el siguiente:

- Creación de redes locales: configuración de dispositivos físicos para la interconexión de equipos informáticos.
- Creación de grupos de usuarios, adjudicación de permisos, y puesta a disposición de contenidos y recursos para su uso en redes locales bajo diferentes sistemas operativos.
- Seguridad en Internet. El correo masivo y la protección frente a diferentes tipos de programas, documentos o mensajes susceptibles de causar perjuicios. Importancia de la adopción de medidas de seguridad activa y pasiva.
- Conexiones inalámbricas e intercambios de información entre dispositivos móviles.

Sin duda es donde podemos encajar de manera más apropiada el tema elegido. Puede ser incorporado a todos los puntos, aunque donde más hincapié haremos es en los puntos 2 y 3.

3.4. Definición de conceptos

A continuación vamos a pasar a definir algunos conceptos básicos que serán expuestos de manera más amplia en el siguiente punto:

- Malware: aquel tipo de software diseñado de manera intencionada para bloquear el funcionamiento normal de cualquier sistema informático, para espiar o acceder a información privada o para acceder de manera ilegítima a sistemas a los que no se tiene permiso, entre otro tipo de conductas abusivas.
- Vulnerabilidad informática: Se trata de un agujero en la seguridad de un sistema informático que permite violar su integridad.
- Ciberdelincuencia: Se trata de acciones antijurídicas que se llevan a cabo por medios informáticos con el objetivo intencionado de acceder a información de manera ilegítima, destrucción de información, bloqueo de sistemas entre otras acciones.
- Herramientas preventivas: Son herramientas que tratan de evitar que se produzcan ataques informáticos.
- Herramientas paliativas: Herramientas que tratan de restaurar y subsanar los daños causados por un ataque informático.

3.5. Antecedentes y estado de la cuestión

A medida que la tecnología ha ido evolucionando y la hemos implicado con más intensidad en nuestra vida diaria, los delitos informáticos han incrementado de manera paralela.

Según DeLooze [3] la creencia de que se puede evitar que existen brechas de seguridad, es algo poco realista, por lo que se debe trabajar para detectarlas y clasificarlas cuando ocurren para tratar de reparar los daños que causan y poder prevenir mayores daños ahora y en el futuro.

3.5.1. Ciberdelincuencia

En 2013, Anderson [4] realizó un estudio para medir el coste de la ciberdelincuencia en Reino Unido y en el resto del mundo. Anderson introduce una primera clasificación, distinguiendo los ciberdelitos que han aparecido como una evolución a través de la tecnología de delitos ya existentes (como la evasión de impuestos, fraudes de tarjeta de crédito, etc.) a los que llama “delitos tradicionales”, de aquellos que deben su propia existencia a Internet, a los que llama “nuevos ciberdelitos”, como puede ser la creación de robots que cometan delitos a través de la red.

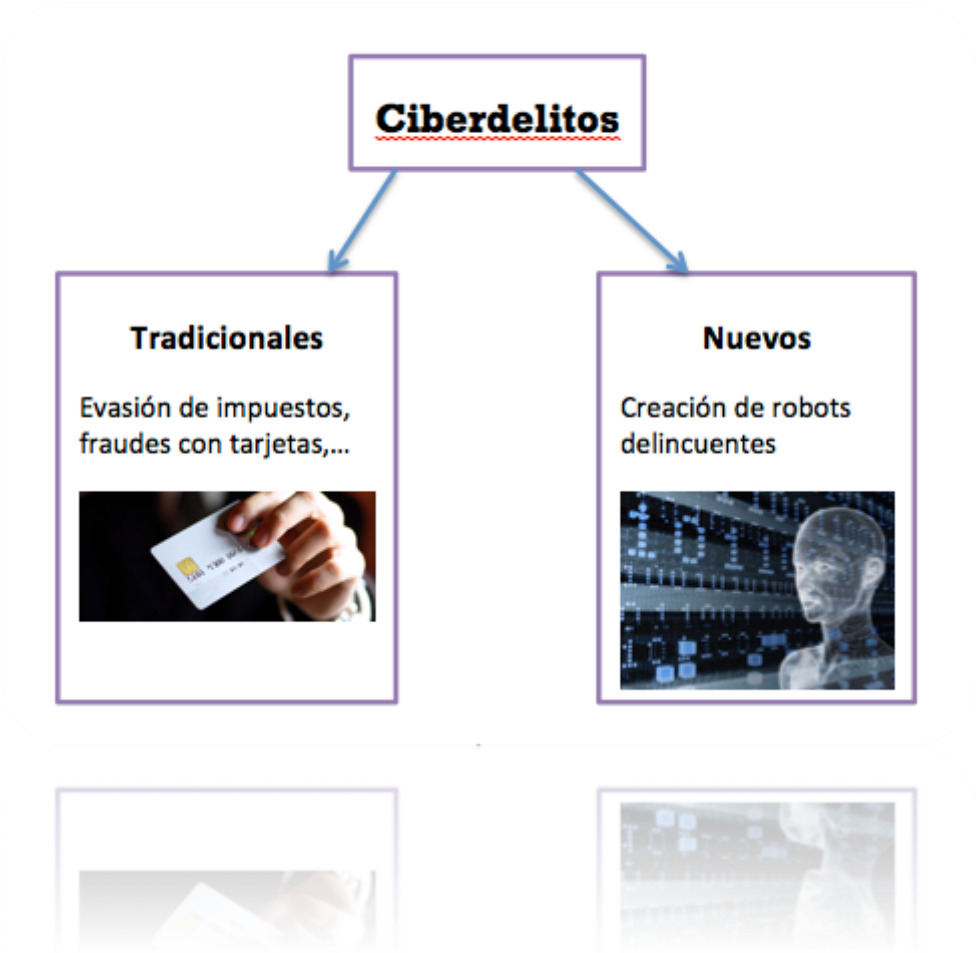


Figura 1. Clasificación de los delitos según Anderson.

Anderson destacó un hecho curioso, y es que mientras los delitos tradicionales cometidos a través de Internet suponían un coste de unos cientos de euros al año por habitante, los nuevos ciberdelitos apenas suponían un coste de unos pocos céntimos de euro por habitante. Sin embargo, los costes indirectos, principalmente destinados a la defensa de este tipo de delitos era proporcionalmente mucho mayor. Anderson muestra el ejemplo de los delitos relacionados con el spam, que en 2010 proporcionaron a los delincuentes alrededor de 2,7 millones de dólares de beneficio, mientras que los costes en la prevención de este tipo de ataques ascendió por encima de los mil millones de dólares, por lo que destaca la ineficiencia que existe en la lucha contra este tipo de delincuencia. Anderson en su trabajo propone invertir menos dinero en medidas de prevención (antivirus, firewalls, etc.), y dedicar mayores esfuerzos en localizar y llevar a prisión a los ciberdelincuentes.

Desde el punto de vista legal, Yar [5] hace una clasificación de cuatro tipos de delitos informáticos.

- Acceso no legítimo: acceso a redes o sistemas privados a los que no se está autorizado.
- Robo: robo de dinero, fraudes con tarjetas de crédito, robo de propiedad intelectual, etc.
- Pornografía: delitos relacionados con la pornografía.
- Violencia: realización de daño físico o psicológico contra otros, o la incitación de la violencia y el odio contra los demás a través de la red.

En este trabajo nos vamos a centrar en los dos primeros, que son los que se pueden clasificar dentro de los ataques informáticos.

La organización sin ánimo de lucro MITRE formada por numerosos centros de investigación y desarrollo y situada en sectores estratégicos y críticos de Estados Unidos como son defensa, inteligencia, sistema sanitario, entre otros, ha desarrollado a lo largo del tiempo una lista pública con información detallada sobre vulnerabilidades en la seguridad conocidas. Sin embargo, según DeLooze [3], la lista del MITRE está organizada según un criterio temporal, de acuerdo al orden en el que han ido siendo reconocidas las vulnerabilidades. DeLooze propone una organización según un mapa organizativo para crear perfiles que nos permitan clasificarlos según sus características. Este hecho facilitaría localizar un ataque, y ayudaría a mitigar los efectos de un ataque aplicando las políticas que se hayan aplicado en situaciones similares. Así, DeLooze, clasifica los tipos de ataque según una taxonomía que divide las amenazas entre las cuatro grandes categorías, y el mapa organizativo expuesto anteriormente.

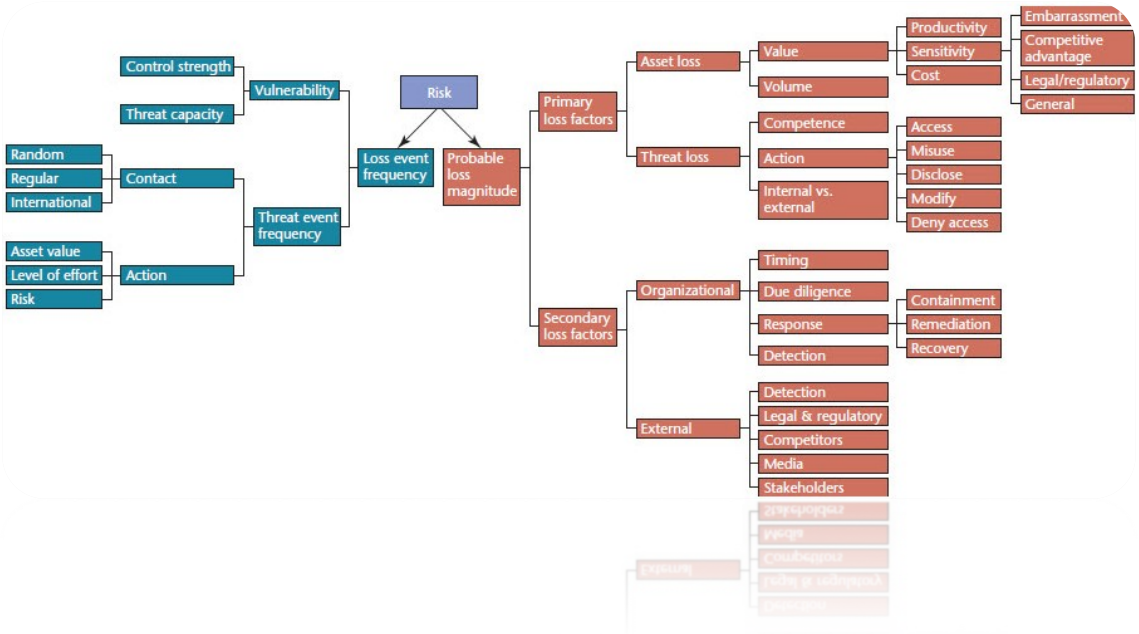


Figura 2. Posible Mapa taxonómico de riesgos en una organización. [6]

3.5.2. Ataques Informáticos y Software Malicioso

Según un informe publicado por Symantec en 2008, el número de códigos maliciosos que había en el mundo habría superado al de aplicaciones legítimas [7]. Según ese mismo informe, sólo en el año 2007 se había producido tanto malware como en los 20 años anteriores juntos, y la tendencia de crecimiento exponencial no parece frenarse. De acuerdo con otro informe publicado en enero de 2015 por la empresa AV-Test, podemos ver que la tasa de crecimiento de esta tendencia ha aumentado en los últimos 4 años como se puede apreciar en la siguiente gráfica:

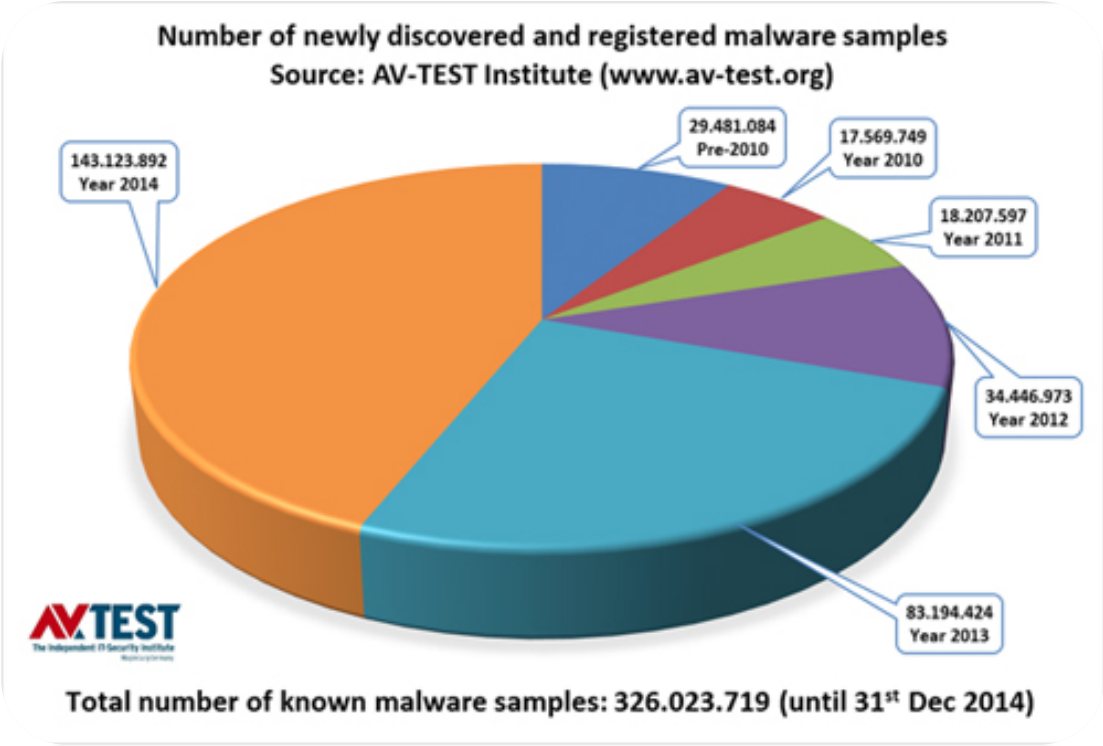


Figura 3. Número de nuevas amenazas descubiertas al año entre 2010 y 2014. Fuente AV-Test [17]

Según otro estudio realizado por G Data's [18] podemos observar igualmente esa tendencia de crecimiento exponencial en la creación de nuevos tipos de malware, habiéndose casi doblado entre 2013 y 2014.

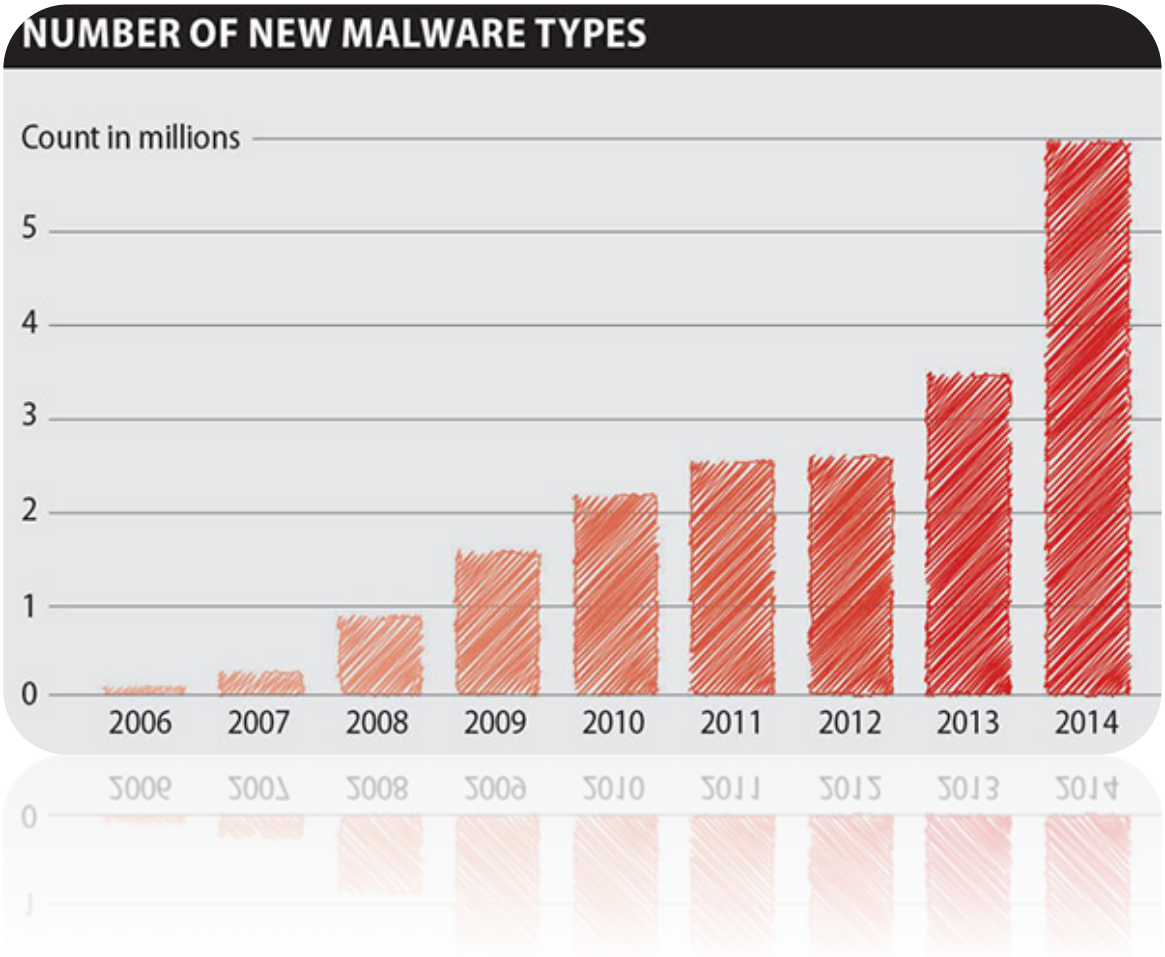


Figura 4. Número de nuevos tipos de malware.

A la vista de los datos, la seguridad de un sistema informático no es una cuestión que debiera tratarse de manera trivial, y ya que como dice DeLooze en su trabajo [3] intentar evitar que existan brechas de seguridad en un sistema es un hecho irreal, y según algunos autores incluso imposible, es importante conocer los tipos de amenazas que existen, clasificarlos, medir y tratar de minimizar sus daños y establecer procedimientos de actuación cuando se sufre un ataque.

Pero, ¿qué es el malware? El malware puede ser definido como aquel tipo de software diseñado de manera intencionada para bloquear el funcionamiento normal de cualquier sistema informático, para espiar o acceder a información privada o para acceder de manera ilegítima a sistemas a los que no se tiene permiso, entre otro tipo de conductas abusivas [8].

Tipos de malware y amenazas

Vamos a pasar a describir los tipos de software malintencionado que existen [9]:

- Virus: Se trata del tipo de software malintencionado más conocido y a menudo se confunden con otros tipos de malware. No todos los malware son virus. Son un tipo de software con la capacidad de infectar el software que exista en el sistema informático y que realizan acciones perjudiciales, como el borrado o la modificación de archivos del sistema.
- Gusanos: A diferencia de los virus, tienen además la capacidad de aprovechar vulnerabilidades para transmitirse a través de redes de unos ordenadores a otros. La principal diferencia entre ambos es que los virus necesitan la intervención de un usuario, mientras que el gusano se transmite de manera automática [10].
- Backdoor: Consiste en la creación de procedimientos para eludir los métodos de autenticación para el acceso a un sistema informático, que permite la instalación de una puerta trasera que facilite a los atacantes el acceso al sistema en el futuro [11].
- Rootkits: Se trata de código que se encarga de alterar el sistema operativo para evitar ser detectado por el sistema. [12].
- Troyanos: Consisten en programas que aparentemente pueden parecer atractivos para el usuario, lo que incita a que éste lo ejecute, y desde ese momento, el software permite realizar acciones maliciosas como el control remoto, el borrado o alteración de ficheros entre otras [13]. Suelen ser la forma de inicializar los gusanos u otros tipos de malware.
- Phishing: Se trata de un modelo con el que se consigue información de manera fraudulenta de un usuario, como pueden ser contraseñas, mediante el engaño haciéndose pasar por una persona o entidad que en realidad no es [16].
- Hijackers: Se trata de software con capacidad para redireccionar a través de cambios en la configuración de los navegadores de Internet, así como de ficheros hosts o DNS que hacen que un usuario sea redirigido a páginas falsas sin que éste pueda advertirlo. Su objetivo es obtener información como contraseñas de acceso a servicios y en casos más graves para el robo de datos financieros o de tarjetas de crédito.
- Keyloggers: En este punto encontramos programas que monitorizan el teclado, almacenándolas en bases de datos para conseguir información privada que permita el acceso a información financiera.
- Stealers: Son programas que permiten robar la información almacenada en los navgadores, como contraseñas y otra información sensible.
- Botnets: Se trata de un número de ordenadores conectados a una red, controlados por una única máquina y que permite realizar acciones maliciosas a través de todos esos equipos, como el envío masivo de spam [14].

- Software de rescate falso: En este punto podemos encontrar el software de tipo rogue, que le crea al usuario la idea de que está infectado por algún tipo de malware y que necesita un tipo de antivirus que le permita dehacerse de él, para lo cual debe pagar una cantidad. Mientras que los Ransomware cifran archivos importantes del sistema y obligan al usuario a pagar una cantidad por liberarlos.
- Adware: Es cualquier tipo de software que de manera automática muestra publicidad a través de un programa como un navegador de internet o un reproductor multimedia, siendo molesto, aunque en la mayoría de las ocasiones no supone un conflicto grave con la seguridad de los sistemas. A menudo se instalan sin que el usuario se dé cuenta, junto a otros programas que ha instalado de manera consciente.
- Spyware: Es cualquier tipo de software que recopila, sin su consentimiento, información del usuario, como datos de sitios a los que accede, y que genera bases de datos que permiten enviar spam relacionado con los gustos del usuario.
- RAM scraper: Los sistemas de pago por tarjeta son sistemas de una extrema seguridad en sus comunicaciones, sin embargo, hay un pequeño instante en que los datos que se mueven en estos sistemas son vulnerables. Se trata del instante en que la información que maneja (por ejemplo la clave de nuestra tarjeta de crédito) es almacenada en una memoria de tipo RAM del dispositivo en el que se introduce una tarjeta de crédito justo antes de ser encriptada y enviada. Los sistemas RAM scraper tratan de explotar esta vulnerabilidad.
- Ingeniería social: Consiste en obtener información que permita el acceso a sistemas, a través de engaños o investigando información del usuario. Esta amenaza explota el hecho de que en un sistema de seguridad el usuario suele ser el eslabón más débil.
- Ataques de fuerza bruta: Consiste en un ataque que trata de encontrar la clave de un sistema probando todas las combinaciones posibles.

En el siguiente gráfico obtenido de un informe de Verizon [20], podemos ver la evolución que han tenido los tipos de ataques informáticos en el periodo de 2010 – 2014 en porcentaje.

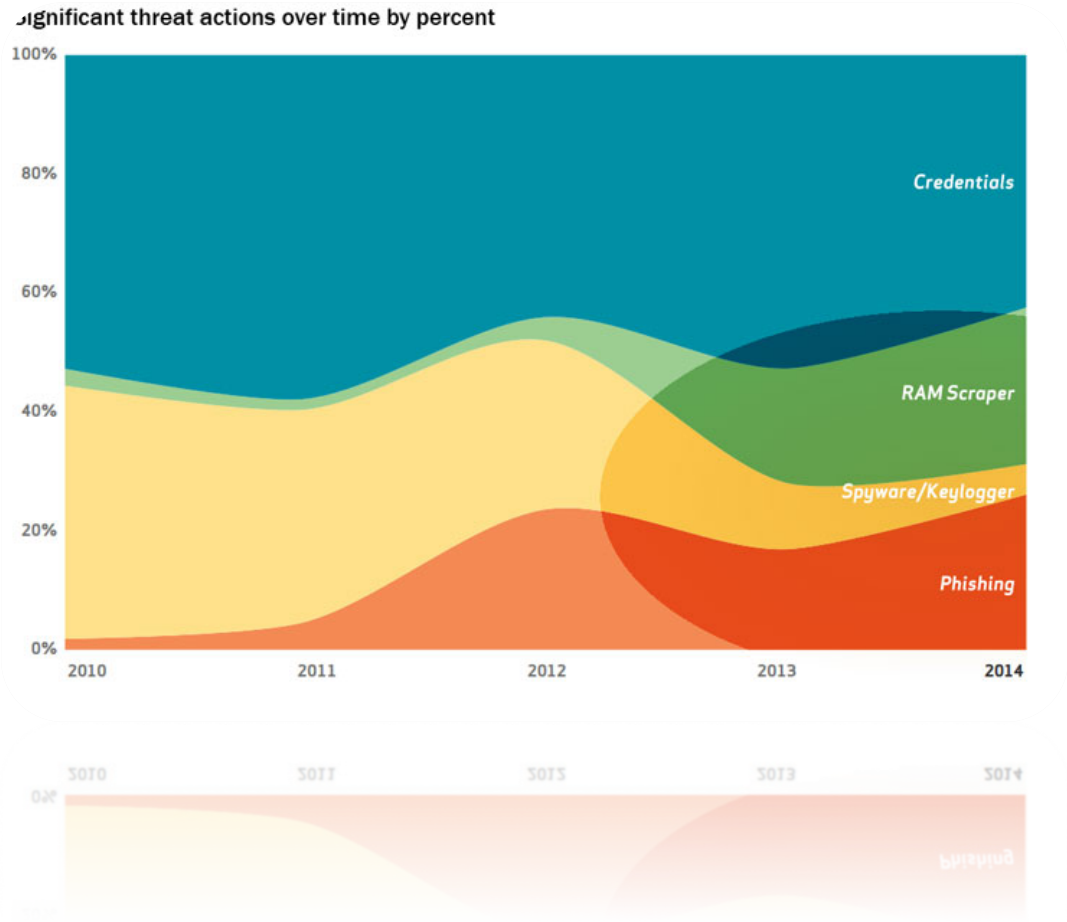


Figura 5. Porcentaje de tipos de ataques

En el gráfico podemos observar el sorprendente ascenso de los ataques de tipo RAM scraper desde 2012, así mismo, podemos observar como el phishing ha crecido a medida que los spyware y keylogger han ido disminuyendo. Siguen siendo los más comunes los relacionados con credenciales de usuarios comprometidas ya sea por ingeniería social, o por cualquier tipo de malware.

3.5.3. Herramientas preventivas y paliativas

Es generalizado el referirse a cualquier tipo de malware como virus informático. Es por ello que todas las herramientas destinadas tanto a la prevención como a la subsanación de los fallos provocados por los posibles ataques de un malware se hagan llamar antivirus. Por esta razón, a pesar de que vamos a referirnos a estas herramientas como antivirus, nos estamos refiriendo a cualquier tipo de herramienta encaminada a frenar la acción de todo tipo de malware [21].

Antivirus

Los antivirus nacieron con el objetivo detectar y eliminar virus informáticos. Con la evolución de Internet los programas han ido evolucionando para combatir otro tipo de amenazas como spyware, gusanos, troyanos, rootkits, adware, etc.

Existen varios tipos de antivirus que pasaremos a describir a continuación:

- Preventivos: se encargan de prevenir cualquier tipo de infección de malware. Se encargan de monitorizar el ordenador: su memoria, disco duro, tráfico, etc.
- Identificativos: Se encargan de localizar determinado software que tienen reconocidos como malignos en sus bases de datos.
- Cortafuegos: Se encargan de bloquear el accesos no autorizados a los sistemas informáticos, debiendo identificar el acceso que sí está permitido para no bloquearlo. Pueden ser implementados mediante hardware o software o mediante una combinación de ambos. Todo el tráfico que haya en la red, debe pasar forzosamente por el firewall [22].
- Antispyware: Se encargan de descubrir los programas que de manera oculta al usuario, están espiando su actividad, y recabando información con fines de explotarla comercialmente.
- Antiadware: Su objetivo es localizar los programas que se han instalado sin conocimiento del usuario y que se encargan de mostrar anuncios no deseados.
- Antispam: Son sistemas que suelen tener principalmente los servidores de correo para manejar el spam y descartar los mensajes que previsiblemente no son deseados por parte del usuario [23].
- Comparación de archivos: se trata de sistemas que ya sea por firmas, por métodos heurísticos o por firmas de archivos en forma de vacuna, identifican archivos que han sido modificados y los ponen en cuarentena por si la modificación del programa implica una acción de malware.

Copias de seguridad

Las copias de seguridad son una herramienta paliativa, ya que se recurre a ellas cuando un malware ha actuado de manera maliciosa en un sistema. Con ellas se trata de restaurar un sistema a un punto anterior de que el malware llevara a cabo su acción (ya fuera borrado, o modificación de archivos).

Es importante establecer una política de copias de seguridad correcta, decidiendo qué elementos son críticos, seleccionando los ficheros a mantener en nuestras copias, y la frecuencia con la que han de hacerse.

Las copias de seguridad deben ser una estrategia complementaria a todos las herramientas de prevención de malware que hemos visto en el punto anterior, ya que su efecto es meramente restaurador, y deberían ser utilizadas en última instancia,

cuando todo nuestro sistema preventivo ha fallado al encontrarse una brecha de seguridad en el mismo [24].

En la siguiente figura vamos a ver un gráfico de la empresa Choice Network en la que muestran su sistema (estrategia) de seguridad:

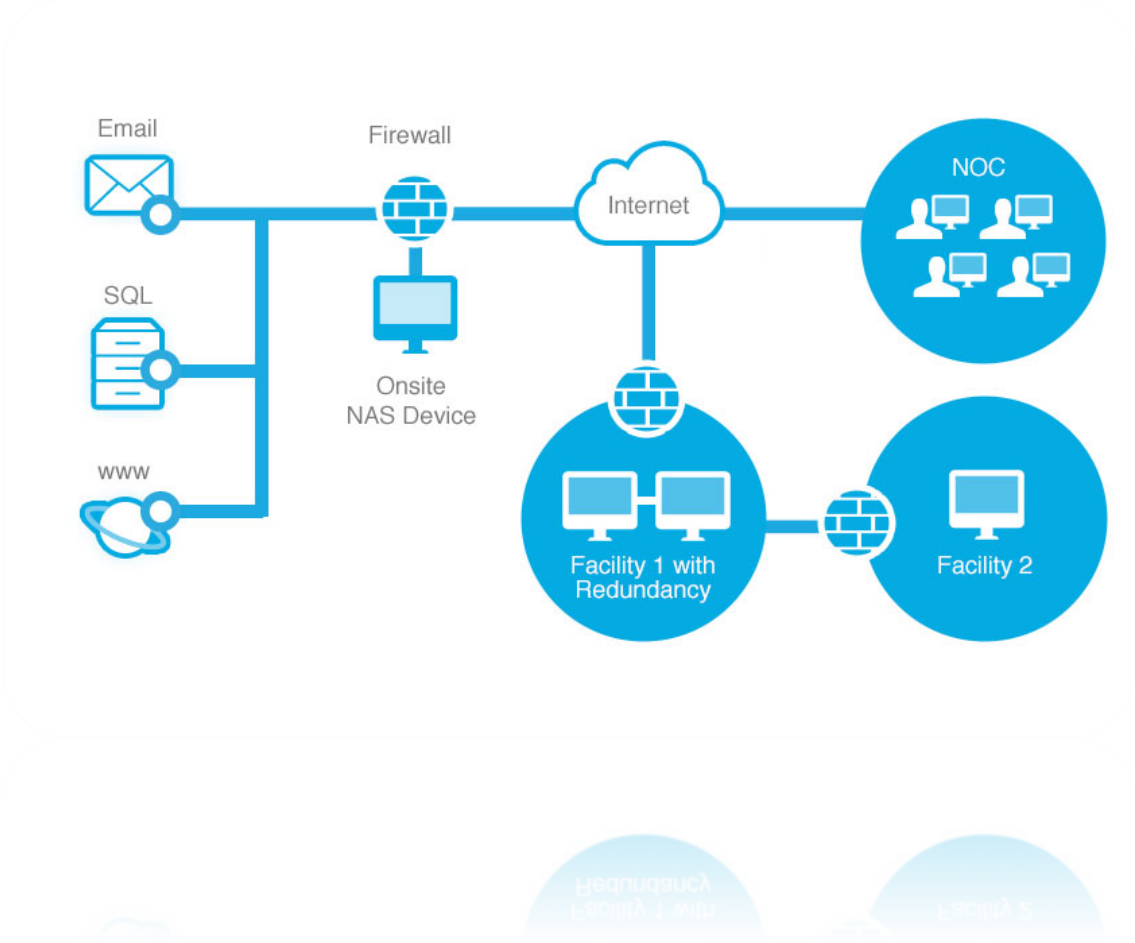


Figura 6. Sistema de seguridad de la empresa Choice Networks

En él podemos ver que sus servicios (correo, base de datos y páginas web, se encuentra accesible a través de Internet, pasando por un cortafuegos (primer elemento de seguridad). Además dispone de dos localizaciones externas donde dispone de los datos de manera redundada, con sendos cortafuegos (que permitiría restaurar el sistema en caso de un ataque al sistema original).

3.5.4. Estado del arte

En los últimos años la computación ha evolucionado hacia la nube. Este sistema que ha revolucionado la computación en el sentido de haber conseguido una abstracción en

infraestructuras remotas a un bajo coste, también ha planteado unos retos en lo que a seguridad y privacidad concierne [25].

La seguridad en la nube todavía se encuentra en una fase muy inicial. Se trata de un tema clave, debido a la cantidad de información que los sistemas manejan, y a los riesgos en la privacidad y en la seguridad de esa información cuando viaja a través de su infraestructura [26].

La seguridad en los sistemas en la nube es todavía a día de hoy un reto muy importante sobre el que se está trabajando profundamente. Sólo tenemos que echar un vistazo al esfuerzo que dedican a este tema empresas como Dropbox [27].

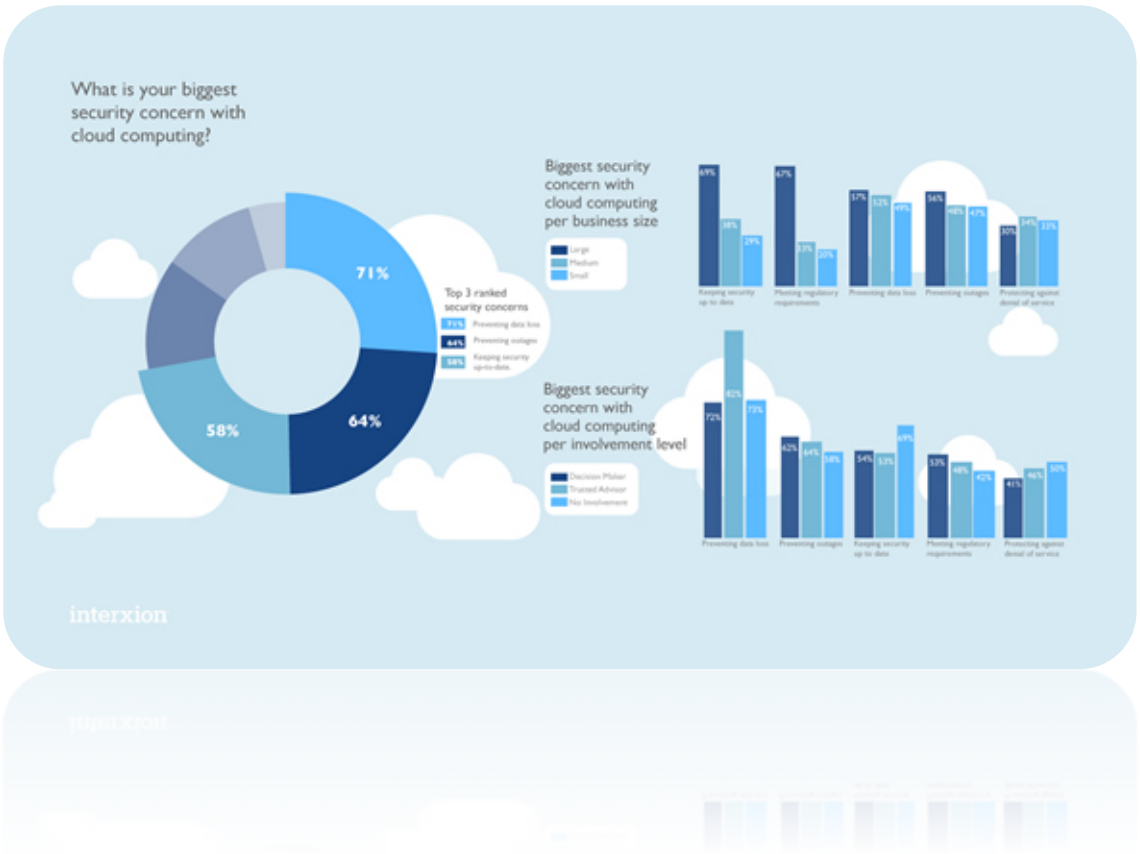


Figura 7. Mayores preocupaciones de los usuarios en la computación en la nube.

3.6. Definición de los conceptos y establecimiento de objetivos.

Una vez realizado el estudio de la cuestión, se establecen los siguientes conceptos como claves para que el alumnado aprenda a lo largo de la unidad didáctica:

- Vulnerabilidades
- Malware
- Ciberdelincuencia

- Herramientas preventivas y paliativas: Antivirus y copias de seguridad
- Políticas de seguridad
- Amenazas
- Ciberdelitos

Y planteamos como objetivos que el alumnado deberá:

- Entender que cualquier sistema puede tener vulnerabilidades.
- Saber que hay que establecer políticas de actuación, clasificación y evaluación frente amenazas aunque se haya invertido en evitar que haya brechas de seguridad. Ningún sistema puede tener una garantía 100% de que no tenga agujeros en su seguridad.
- Conocer y clasificar los tipos de malware y de amenazas que existen y cómo actuar para evitarlas y para subsanar sus consecuencias cuando ocurren.
- Entender que esas amenazas están en constante evolución y pueden surgir nuevas con la evolución de la tecnología.
- Saber establecer protocolos de seguridad en un sistema informático.
- Conocer y clasificar los distintos tipos de herramientas que existen para prevenir un ataque y para corregir las consecuencias.

3.7. Enfoque didáctico

La proyección didáctica del tema, será enfocada de una manera muy práctica. La intención es que el alumnado asimile claramente la importancia de la seguridad en los sistemas informáticos y las consecuencias que puede tener una mala política de seguridad en todos los niveles (personal, institucional, e incluso a nivel de organizaciones públicas y estados).

Además se fomentará un espíritu crítico del alumnado a la hora de valorar las consecuencias que pueden tener los actos que se llevan a través de Internet, siendo extrapolables a la vida diaria.

Se enfocará de la siguiente manera: Se realizará un juego de roles, para lo que se crearán grupos compuestos de varios alumnos y alumnas. Cada grupo representará una institución, empresa, familia, grupos de ciberdelincuentes, grupos de amigos, personas individuales, etc. Todos estos grupos formarán en su conjunto, una comunidad en la que los actos que unos realicen tengan consecuencias sobre otros. La actividad irá dirigida por el profesor, que asignará los papeles y los objetivos de cada uno de los grupos.

Al final de la actividad cada grupo deberá explicar en qué ha consistido su papel, qué consecuencias ha tenido en su grupo, en sí mismo, en otros grupos y en la comunidad en su conjunto.

De esta manera se espera que cada grupo, no sólo sea capaz de clasificar y reconocer los tipos de vulnerabilidades que existen, sino que además puedan entender claramente las consecuencias que podrían tener en sus vidas y en las de las demás personas, con lo que se espera contribuir a la competencia social y ciudadana.

La autonomía que se concede a los grupos, fomentará la adquisición de la competencia en autonomía e iniciativa personal para alcanzar los objetivos que les son asignados.

A la adquisición de la competencia para aprender a aprender se contribuye decisivamente mediante la capacidad desarrollada a través de este enfoque teniendo que obtener información, realizando acciones y comunicando lo aprendido poniéndolo en común con las demás personas.

Además, por la propia naturaleza del tema y de la materia, la competencia en el tratamiento de la información y competencia digital está cubierta.

Algunos de los grupos tendrán que valerse de heurísticas para la consecución de sus objetivos (por ejemplo para romper una clave, o para hacer una clave segura), contribuyendo a la competencia matemática.

Por otro lado, se trabajará la competencia lingüística durante la búsqueda de la información necesaria para el desarrollo del tema y que en ocasiones será incluso en más de un idioma, además de tener que hacer una presentación en la que practicarán y mejoraran su manera de desenvolverse y de expresarse.

Puesto que se tratarán casos en los que se atente contra la igualdad, se abarcará también el tema de la igualdad que será debatido.

Otro de los temas transversales que será cubierto será el de la ética informática. El debate que se abrirá después de la actividad permitirá analizar uno a uno todos los actos que se han realizado con el que se pretende que el alumnado recoja una actitud crítica y sepa distinguir entre la legalidad y la ética de sus actos.

4. Proyección didáctica

La legislación tenida en cuenta para esta proyección didáctica ha sido la Ley Orgánica 2/2006 conocida como Ley Orgánica de Educación vigente desde el curso académico 2006/2007 [19].

Esta proyección ha sido desarrollada para la asignatura de Informática del cuarto curso de Educación Secundaria Obligatoria.

4.1. Elementos curriculares básicos:

Los siguientes elementos curriculares han sido extraídos de la LOE a través del REAL DECRETO 1631/2006, de 29 de diciembre, por el que se establecen las enseñanzas mínimas correspondientes a la Educación Secundaria Obligatoria [2].

Contribución de la materia a la adquisición de las competencias básicas

Esta materia contribuye de manera plena a la adquisición de la competencia referida a Tratamiento de la información y competencia digital, imprescindible para desenvolverse en un mundo que cambia, y nos cambia, empujado por el constante flujo de información generado y transmitido mediante unas tecnologías de la información cada vez más potentes y omnipresentes.

En la sociedad de la información, las tecnologías de la información y la comunicación ofrecen al sujeto la posibilidad de convertirse en creador y difusor de conocimiento a través de su comunicación con otros sujetos interconectados por medio de redes de información. La adaptación al ritmo evolutivo de la sociedad del conocimiento requiere que la educación obligatoria dote al alumno de una competencia en la que los conocimientos de índole más tecnológica se pongan al servicio de unas destrezas que le sirvan para acceder a la información allí donde se encuentre, utilizando una multiplicidad de dispositivos y siendo capaz de seleccionar los datos relevantes para ponerlos en relación con sus conocimientos previos, y generar bloques de conocimiento más complejos. Los contenidos de la materia de Informática contribuyen en alto grado a la consecución de este componente de la competencia.

Sobre esta capa básica se solapa el desarrollo de la capacidad para integrar las informaciones, reelaborarlas y producir documentos susceptibles de comunicarse con los demás en diversos formatos y por diferentes medios, tanto físicos como telemáticos. Estas actividades implican el progresivo fortalecimiento del pensamiento crítico ante las producciones ajenas y propias, la utilización de la creatividad como ingrediente esencial en la elaboración de nuevos contenidos y el enriquecimiento de las destrezas comunicativas adaptadas a diferentes contextos. Incorporar a los

comportamientos cotidianos el intercambio de contenidos será posible gracias a la adopción de una actitud positiva hacia la utilización de las tecnologías de la información y la comunicación. Esa actitud abierta, favorecida por la adquisición de conductas tendentes a mantener entornos seguros, permitirá proyectar hacia el futuro los conocimientos adquiridos en la fase escolar. Dicha proyección fomentará la adopción crítica de los avances tecnológicos y las modificaciones sociales que éstos produzcan.

Desde este planteamiento, los conocimientos de tipo técnico se deben enfocar al desarrollo de destrezas y actitudes que posibiliten la localización e interpretación de la información para utilizarla y ampliar horizontes comunicándola a los otros y accediendo a la creciente oferta de servicios de la sociedad del conocimiento, de forma que se evite la exclusión de individuos y grupos. De esta forma se contribuirá de forma plena a la adquisición de la competencia, mientras que centrarse en el conocimiento exhaustivo de las herramientas no contribuiría sino a dificultar la adaptación a las innovaciones que dejarían obsoleto en un corto plazo los conocimientos adquiridos.

Además, la materia contribuye de manera parcial a la adquisición de la competencia cultural y artística en cuanto que ésta incluye el acceso a las manifestaciones culturales y el desarrollo de la capacidad para expresarse mediante algunos códigos artísticos. Los contenidos referidos al acceso a la información, que incluye las manifestaciones de arte digital y la posibilidad de disponer de informaciones sobre obras artísticas no digitales inaccesibles físicamente, la captación de contenidos multimedia y la utilización de aplicaciones para su tratamiento, así como la creación de nuevos contenidos multimedia que integren informaciones manifestadas en diferentes lenguajes colaboran al enriquecimiento de la imaginación, la creatividad y la asunción de reglas no ajenas a convenciones compositivas y expresivas basadas en el conocimiento artístico.

La contribución a la adquisición de la competencia social y ciudadana se centra en que, en tanto que aporta destrezas necesarias para la búsqueda, obtención, registro, interpretación y análisis requeridos para una correcta interpretación de los fenómenos sociales e históricos, permite acceder en tiempo real a las fuentes de información que conforman la visión de la actualidad. Se posibilita de este modo la adquisición de perspectivas múltiples que favorezcan la adquisición de una conciencia ciudadana comprometida en la mejora de su propia realidad social. La posibilidad de compartir ideas y opiniones a través de la participación en redes sociales, brinda unas posibilidades insospechadas para ampliar la capacidad de intervenir en la vida ciudadana, no siendo ajena a esta participación el acceso a servicios relacionados con la administración digital en sus diversas facetas.

La contribución a la adquisición de la competencia para aprender a aprender está relacionada con el conocimiento de la forma de acceder e interactuar en entornos virtuales de aprendizaje, que capacita para la continuación autónoma del aprendizaje una vez finalizada la escolaridad obligatoria. En este empeño contribuye decisivamente la capacidad desarrollada por la materia para obtener información, transformarla en conocimiento propio y comunicar lo aprendido poniéndolo en común con los demás.

Contribuye de manera importante en la adquisición de la competencia en comunicación lingüística, especialmente en los aspectos de la misma relacionados con el lenguaje escrito y las lenguas extranjeras. Desenvolverse ante fuentes de información y situaciones comunicativas diversas permite consolidar las destrezas lectoras, a la vez que la utilización de aplicaciones de procesamiento de texto posibilita la composición de textos con diferentes finalidades comunicativas. La interacción en lenguas extranjeras colaborará a la consecución de un uso funcional de las mismas.

Contribuye de manera parcial a la adquisición de la competencia matemática, aportando la destreza en el uso de aplicaciones de hoja de cálculo que permiten utilizar técnicas productivas para calcular, representar e interpretar datos matemáticos y su aplicación a la resolución de problemas. Por otra parte, la utilización de aplicaciones interactivas en modo local o remoto, permitirá la formulación y comprobación de hipótesis acerca de las modificaciones producidas por la modificación de datos en escenarios diversos.

A la adquisición de la competencia en el conocimiento y la interacción con el mundo físico, se contribuye en tanto que proporciona destrezas para la obtención de información cualitativa y cuantitativa que acepte la resolución de problemas sobre el espacio físico. La posibilidad de interactuar con aplicaciones de simulación que permitan observar procesos, cuya reproducción resulte especialmente dificultosa o peligrosa, colabora igualmente a una mejor comprensión de los fenómenos físicos.

Por último, contribuye a la competencia de autonomía e iniciativa personal en la medida en que un entorno tecnológico cambiante exige una constante adaptación. La aparición de nuevos dispositivos y aplicaciones asociadas, los nuevos campos de conocimiento, la variabilidad de los entornos y oportunidades de comunicación exigen la reformulación de las estrategias y la adopción de nuevos puntos de vista que posibiliten resolución de situaciones progresivamente más complejas y multifacéticas.

Objetivos

La enseñanza de la Informática en esta etapa tendrá como finalidad el desarrollo de las siguientes capacidades:

Utilizar los servicios telemáticos adecuados para responder a necesidades relacionadas, entre otros aspectos, con la formación, el ocio, la inserción laboral, la administración, la salud o el comercio, valorando en qué medida cubren dichas necesidades y si lo hacen de forma apropiada.

Buscar y seleccionar recursos disponibles en la red para incorporarlos a sus propias producciones, valorando la importancia del respeto de la propiedad intelectual y la conveniencia de recurrir a fuentes que autoricen expresamente su utilización.

Conocer y utilizar las herramientas para integrarse en redes sociales, aportando sus competencias al crecimiento de las mismas y adoptando las actitudes de respeto, participación, esfuerzo y colaboración que posibiliten la creación de producciones colectivas.

Utilizar periféricos para capturar y digitalizar imágenes, textos y sonidos y manejar las funcionalidades principales de los programas de tratamiento digital de la imagen fija, el sonido y la imagen en movimiento y su integración para crear pequeñas producciones multimedia con finalidad expresiva, comunicativa o ilustrativa.

Integrar la información textual, numérica y gráfica para construir y expresar unidades complejas de conocimiento en forma de presentaciones electrónicas, aplicándolas en modo local, para apoyar un discurso, o en modo remoto, como síntesis o guión que facilite la difusión de unidades de conocimiento elaboradas.

Integrar la información textual, numérica y gráfica obtenida de cualquier fuente para elaborar contenidos propios y publicarlos en la Web, utilizando medios que posibiliten la interacción (formularios, encuestas, bitácoras, etc.) y formatos que faciliten la inclusión de elementos multimedia decidiendo la forma en la que se ponen a disposición del resto de usuarios.

Conocer y valorar el sentido y la repercusión social de las diversas alternativas existentes para compartir los contenidos publicados en la web y aplicarlos cuando se difundan las producciones propias.

Y por último, a los dos siguientes puntos serán a los que de manera más específica contribuirá para su consecución el tema elegido en este trabajo:

Adoptar las conductas de seguridad activa y pasiva que posibiliten la protección de los datos y del propio individuo en sus interacciones en Internet.

Valorar las posibilidades que ofrecen las tecnologías de la información y la comunicación y las repercusiones que supone su uso.

Contenidos

Bloque 1. Sistemas operativos y seguridad informática.

Creación de redes locales: configuración de dispositivos físicos para la interconexión de equipos informáticos.

Creación de grupos de usuarios, adjudicación de permisos, y puesta a disposición de contenidos y recursos para su uso en redes locales bajo diferentes sistemas operativos.

Seguridad en Internet. El correo masivo y la protección frente a diferentes tipos de programas, documentos o mensajes susceptibles de causar perjuicios. Importancia de la adopción de medidas de seguridad activa y pasiva.

Conexiones inalámbricas e intercambios de información entre dispositivos móviles.

Bloque 2. Multimedia.

Adquisición de imagen fija mediante periféricos de entrada.

Tratamiento básico de la imagen digital: los formatos básicos y su aplicación, modificación de tamaño de las imágenes y selección de fragmentos, creación de dibujos sencillos, alteración de los parámetros de las fotografías digitales: saturación, luminosidad y brillo.

Captura de sonido y vídeo a partir de diferentes fuentes.

Edición y montaje de audio y vídeo para la creación de contenidos multimedia.

Las redes de intercambio como fuente de recursos multimedia. Necesidad de respetar los derechos que amparan las producciones ajenas.

Bloque 3. Publicación y difusión de contenidos.

Integración y organización de elementos textuales, numéricos, sonoros y gráficos en estructuras hipertextuales.

Diseño de presentaciones.

Creación y publicación en la Web. Estándares de publicación.

Accesibilidad de la información.

Bloque 4. Internet y redes sociales.

La información y la comunicación como fuentes de comprensión y transformación del entorno social: comunidades virtuales y globalización.

Actitud positiva hacia las innovaciones en el ámbito de las tecnologías de la información y la comunicación y hacia su aplicación para satisfacer necesidades personales y grupales.

Acceso a servicios de administración electrónica y comercio electrónico: los intercambios económicos y la seguridad.

Acceso a recursos y plataformas de formación a distancia, empleo y salud.

La propiedad y la distribución del «software» y la información: «software» libre y «software» privativo, tipos de licencias de uso y distribución.

La ingeniería social y la seguridad: estrategias para el reconocimiento del fraude, desarrollo de actitudes de protección activa ante los intentos de fraude.

Adquisición de hábitos orientados a la protección de la intimidad y la seguridad personal en la interacción en entornos virtuales: acceso a servicios de ocio.

Canales de distribución de los contenidos multimedia: música, vídeo, radio, TV.

Acceso, descarga e intercambio de programas e información. Diferentes modalidades de intercambio.

La materia elegida, se encuadra dentro del bloque 1 de la asignatura, en concreto en el punto:

Seguridad en Internet. El correo masivo y la protección frente a diferentes tipos de programas, documentos o mensajes susceptibles de causar perjuicios. Importancia de la adopción de medidas de seguridad activa y pasiva.

4.2. Metodología

Para el desarrollo de esta unidad didáctica se va a emplear una mezcla de metodología basada en proyecto y aprendizaje cooperativo. Se trata en ambos casos de una metodología activa en la que el alumnado no se limita a recibir información de forma pasiva, sino que se involucra, y se convierte en el protagonista del proceso de aprendizaje en colaboración con sus compañeros fomentando su autonomía, y su mejora en el trabajo en equipo.

El aprendizaje cooperativo permite la planificación y la realización de las actividades en grupo, aceptando las normas que se establezcan y donde se proponen objetivos e intereses propios y comunes con el resto del grupo.

El aprendizaje basado en proyectos [28] es opuesto al modelo de aprendizaje de memoria tradicional, muy útil para trabajar con grupos que muestran habilidades y estilos de aprendizaje muy diversos. Trata de plantear una situación problemática real a un grupo, que tendrá que ser trabajada de forma colaborativa en un proyecto que será diseñado por el propio grupo siguiendo las indicaciones dadas por el profesor, y

donde cada alumno o grupo de alumnos tiene un rol propio con unos objetivos a conseguir.

El alumnado trabaja de forma autónoma aunque el profesor se encargará de la supervisión del proyecto.

Los puntos importantes a destacar en este tipo de metodologías son

- Los objetivos globales del proyecto
- Los objetivos de cada participante o grupo de participantes
- Las instrucciones que cada participante o grupo recibe
- El tipo de evaluación final.

El objetivo que persigue esta metodología es hacer partícipe a todos los miembros del grupo en una tarea común, donde los resultados son aplicables al mundo real y donde puedan ver la utilidad real de lo que aprenden. Además permite introducir de manera sencilla áreas transversales al mismo tiempo que se pueden evaluar otros aspectos puntuales de la asignatura en cuestión y, por supuesto, contribuye a aumentar las habilidades sociales del alumnado (trabajo en equipo, comunicación, etc.).

Temporalización

El tema será llevado a cabo durante 3 semanas y abarcará 9 sesiones de una hora cada una.

Sesiones

Sesión 1: Debate: ¿Es importante la seguridad informática?

La primera sesión tiene como objetivo introducir al alumno en el tema en cuestión y conseguir que sea capaz de percibir el alcance que tiene. Es necesario que entienda la importancia que tiene hoy en día la seguridad informática para salvaguardar nuestra privacidad e incluso nuestra propia seguridad. Para ello se busca abrir un debate moderado por el profesor y en el que se pongan de manifiesto casos famosos conocidos en los que un fallo en la seguridad de un sistema informático ha comprometido a organizaciones enteras e incluso a estados.

Material necesario para la sesión

Para la sesión será necesario material impreso que se entregará al alumnado. Además se necesitará disponer de un proyector y un equipo que reproduzca material multimedia para mostrar el vídeo a los alumnos, y las transparencias donde se plantearán los casos a discutir.

Debate

La clase comenzará con la visualización del siguiente vídeo que pondrá en antecedentes al alumnado:

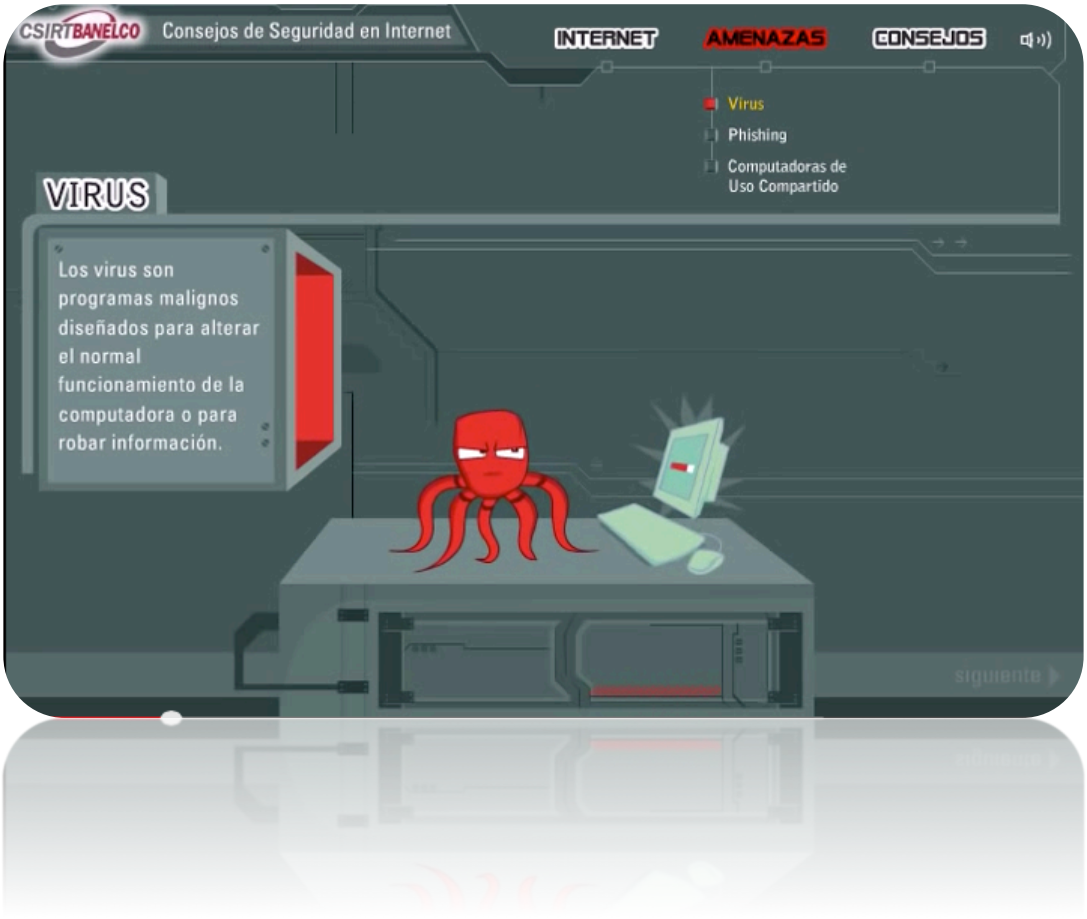


Figura 8. Vídeo para poner en antecedentes al alumnado y sirvan de aproximación al debate que se planteará a continuación.

https://www.youtube.com/watch?v=86cr-EfBz1o#t=72

Inmediatamente entonces empezará el debate que dirigirá el profesor. Cada alumno y alumna recibirá una hoja con una serie de cuestiones generales y que pasarán a debatirse.

Material para el debate

Se empleará la siguiente hoja que será entregada a parejas de alumnos. Se hará en parejas para fomentar el trabajo en equipo, la colaboración y la participación de todos los alumnos y alumnas.

- ¿Qué es la seguridad informática?
- ¿Es importante la seguridad informática?
- ¿Conoces algún caso que haya puesto en riesgo a alguien por culpa de un fallo en la seguridad informática?

- ¿Qué crees que es más importante, invertir mucho tiempo y dinero en tener un sistema a prueba de fallos, o ser flexibles y tener un protocolo de actuación ante un fallo en la seguridad de nuestro sistema?

Se trata de hacer un debate abierto para todos, y entender claramente lo que piensan los alumnos y alumnas, además se intentará que los alumnos sean capaces de tener una actitud crítica y propia ante la cuestión.

Discusión de ejemplos

Con esta actividad se busca que el alumnado se dé cuenta del alcance que puede tener, por pequeño que parezca, un fallo en la seguridad de un sistema informático. Cada caso se presentará junto con una serie de preguntas que se debatirán en clase.

Material para la discusión

El gusano de Morris.

En 1988, Robert Tappan Morris, un estudiante e postgrado, creó un ataque con "gusanos" a gran escala en Internet. Los costos de limpiar el desastre se cifran en 100 millones de dólares. Morris, es hoy profesor del MIT.

¿Por qué creéis que se crea software malicioso?

Heartbleed

En 2014 fue descubierta una vulnerabilidad de primer nivel (que puede ser explotada) en el protocolo de comunicación SSH que comprometía las comunicaciones, correos electrónicos, páginas webs de los usuarios.

¿Existen los sistemas sin fallos?

 **Robo de contraseñas de los hackers rusos** En 2014 un grupo de hackers rusos logró robar más de 1200 millones de contraseñas. ¿Cómo de importante crees que es la manera de guardar la información confidencial?	 Santander **Saludos, respetado cliente!** Seguramente sabrá usted que nuestro banco es una de las más grandes en España y el Grupo Santander forma parte de una de las 10 más grandes bancos en el mundo. Las filiales de nuestra empresa cuentan con representaciones prácticamente en todos los países y su cantidad crece día a día. Santander, con un valor en Bolsa a 31 de diciembre de 2007 de 105.126 millones de euros. En 2007 fueron perfeccionados todos los sistemas de seguridad y fueron puestos en marcha nuevas posibilidades de trabajo con el banco. El equipo de apoyo técnico controla constantemente la funcionalidad de todas las cuentas de nuestros clientes, vigila la seguridad de las cuentas, elimina los problemas que pueden surgir y regula el trabajo del sitio web de Banco Santander. Nuestro grupo técnico ha sido reconocido como el más efectivo en el año 2007 por decisión de expertos en la rama seguridad de la información. Trabajamos arduamente en la modernización del sistema de seguridad de sus cuentas y en la funcionalidad de las mismas, introducimos nuevas tecnologías y ofrecemos además nuevas posibilidades para el trabajo con su cuenta. En enero de este año nuestros especialistas han elaborado un nuevo sistema de confidencialidad y seguridad de sus datos, que protege completamente sus cuentas contra accesos no sancionados y contra el robo de información personal o el dinero. El moderno algoritmo de cifrado ha sido aprobado por los órganos estatales del caso y tienen un 100% de fiabilidad. El sistema elaborado ha pasado exitosamente las pruebas de testeo y la certificación requeridas, y ahora está ya accesible para poder ser instalada en su equipo. Para instalar la actualización del sistema de seguridad, deberá hacerlo desde nuestro sitio web y realizando primero algunos pasos para la activación. La actualización será accesible inmediatamente después de la activación y al primer acceso a su cuenta. **¡Atención!** EL SERVICIO DE APOYO TÉCNICO DE BANCO SANTANDER CENTRAL HISPANO LE RECOMIENDA ENCARECIDAMENTE INSTALAR EL NUEVO SISTEMA DE SEGURIDAD! Al instalar el nuevo sistema, ingrese obligatoriamente sus datos verdaderos, en caso contrario no obtendrá acceso a la actualización. Si Usted tiene una cuenta bancaria personal, pase a la referencia: http://www.gruposantander.es/particulares/ Si Usted tiene una cuenta bancaria corporativa, pase a la referencia: http://www.gruposantander.es/empresas/ Cuando recibes un correo o accedes a un portal financiero, ¿crees que es necesario identificar correctamente que efectivamente esa persona o institución es quien dice ser?

Tabla 1. Tarjetas para debatir[1].

Sesión 2: La vida como un juego

En la sesión 2 se crearán los grupos que participarán en este juego de roles, donde se crearán grupos que representarán organizaciones, empresas, instituciones, grupos de ciberdelincuentes, etc. y donde cada uno tendrá unos objetivos que les serán explicados de forma privada. Igualmente se le entregará una ficha con la explicación y los objetivos de su grupo.

Una vez explicado el papel de cada grupo, se expondrá que la clase entera es una comunidad, donde las acciones de unos grupos tienen consecuencias en la vida de los otros, se estimulará además el interés por querer conocer las consecuencias que van teniendo los actos de unos en otros.

Los grupos a formar serán los siguientes:

- Grupo 1: Estará compuesto por al menos 5 personas y representará a una administración pública. Digamos que será el gobierno de la comunidad. Uno de los componentes (elegido por los componentes del grupo) será el encargado de representar al gobierno ante la comunidad. Su objetivo es velar por el buen funcionamiento de la comunidad, y creará las normas, estableciendo qué está permitido y qué no está permitido.

[1] Las imágenes obtenidas para esta tabla están libres de copyright obtenidas de bancos de imágenes públicos

- Grupo 2: Estará compuesto por al menos 3 personas. Y se encargará de ejercer el papel de policía de la comunidad. Velará por que las normas establecidas por el gobierno se cumplan, y vigilará todo lo que está pasando.
- Grupo 3: Se compondrá de al menos 8 miembros, y se encarga de almacenar el dinero de todos los miembros de la comunidad.
- Grupo 4: Será una importante empresa de software, compuesta por al menos 4 miembros.
- Grupo 5: Se trata de un grupo de ciberdelincuentes que intentará bloquear el sistema de seguridad de la policía y del gobierno para cometer una serie de delitos.
- Grupo 6: Estará compuesto por un solo individuo, que creará un malware, con el ánimo de que se fije en él la empresa de software.
- Grupo 7: Grupo de ciberladrones que intentará robar dinero de las cuentas de toda la comunidad, de la empresa y del gobierno.

Material

Nos valdremos de la plataforma Hacker Expirience (https://hackerexperience.com/) para desarrollar el juego. Además se crearán cuentas de correo electrónico para cada uno de los miembros del grupo. Las fichas a entregar a cada grupo serán:

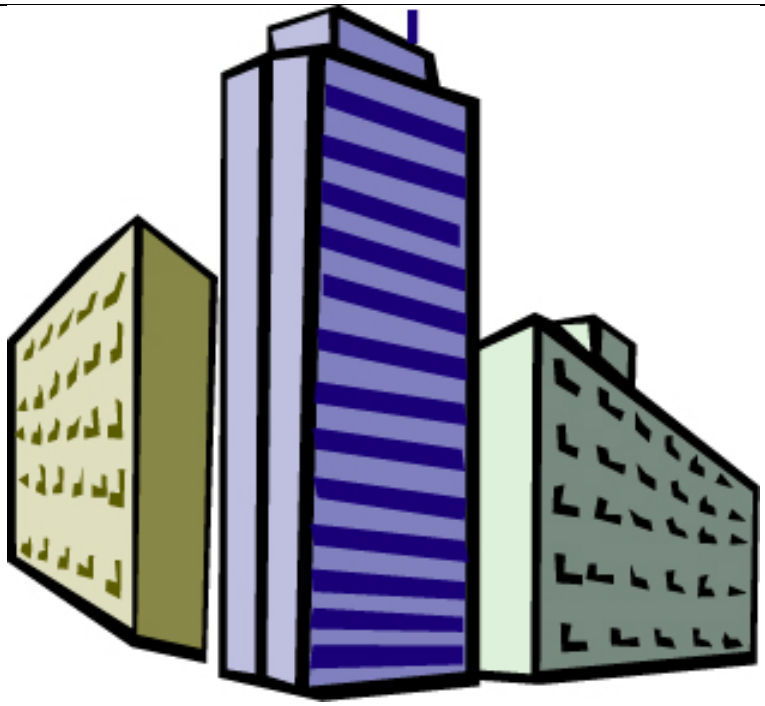
Gobierno: Vuestro grupo se encargará de establecer las normas de la comunidad, es decir, lo que está permitido y lo que no está permitido hacer. Estas normas podrán evolucionar a medida que avanza el juego. Deberéis elegir a un miembro del grupo que represente al gobierno ante el resto de comunidad, para explicar las normas que se establecen. Otro de los miembros del grupo se encargará de gestionar la seguridad del sistema informático propio. Vuestro sistema está desarrollado por la empresa de software del grupo 5, y vuestro dinero lo almacena el banco, por lo que estaréis en continuo contacto con ellos, así como con la policía para velar por el buen funcionamiento de este grupo. Deberéis investigar qué herramientas de prevención de ataques existen, y las herramientas que os ayuden a recuperaros ante un ataque o un fallo en la seguridad de los sistemas informáticos. Además deberéis investigar la legislación vigente en materia de ciberdelincuencia para ayudaros a crear vuestras propias leyes

Policía: Este grupo vela por la seguridad de la comunidad, y por hacer cumplir las normas que establece el gobierno. Uno de los componentes vigilará los sistemas informáticos del grupo, mientras que el resto vigilará las actividades que realizan los demás miembros de la couminidad. Deberéis estar en continua comunicación con el gobierno, además de investigar qué herramientas de prevención de ataques existen, y las herramientas que os ayuden a descubrir posibles fraudes que se estén cometiendo.

Banco: Os encargáis de guardar el dinero de todos los miembros de la comunidad y de

su gestión. Las medidas de seguridad que necesitáis establecer son máximas. Al menos 4 de los miembros deberán establecer las políticas de seguridad que se llevan a cabo, y los otros 4 velarán porque se cumplan. Os encontráis en continua comunicación con la empresa de software que os ha facilitado vuestro sistema de gestión. Deberéis investigar qué herramientas de prevención de ataques existen, y las herramientas que os ayuden a recuperaros ante un ataque o un fallo en la seguridad de los sistemas informáticos.

Empresa: Os dedicáis al desarrollo de software y, entre otros, trabajáis para el banco, el gobierno y la policía, por lo que debéis estar en constante contacto con ellos. Uno de los miembros se dedicará a velar por la seguridad de los sistemas, y los otros por comunicarse con sus clientes. Deberéis investigar qué herramientas de prevención de ataques existen, y las herramientas que os ayuden a recuperaros ante un ataque o un fallo en la seguridad de los sistemas informáticos.



Ciberdelincuentes: Vuestro objetivo es romper los sistemas de seguridad de todos los grupos para cometer vuestros delitos. Deberéis investigar en qué consiste el phishing, el malware, los ataques DoS, y la ingeniería social para conseguir vuestros objetivos.

Hacker: Tu objetivo será crear un tipo de malware que llame la atención a la empresa de software para que te fichen por lo brillante informático que crees que eso te hará parecer. Debes investigar qué tipos de malware hay, diseñar uno y desarrollarlo.

Ciberladrones: Vuestro objetivo es robar todo el dinero que podáis de los demás miembros de la comunidad. Investigad lo que es el phisinig entre otras técnicas de fraude electrónico, como la ingeniería social, etc. Para conseguir vuestros objetivos. Sed cautelosos para no hacer saltar las alarmas de la policía y así podáis pasar desapercibidos.

Tabla 2. Fichas para repartir a cada grupo.[2]

[2] Las imágenes obtenidas para esta tabla están libres de copyright obtenidas de bancos de imágenes públicos

Una vez entregada la ficha a cada grupo se explicará a toda la clase lo siguiente:

"Existe un gobierno que establece las normas del grupo. El gobierno tiene un representante que será el que comunicará las normas. Cada miembro del gobierno tiene un método a través del cual se puede contactar con él y que se pondrá en conocimiento de toda la clase. Además existe un grupo de la policía que vela por el cumplimiento de las normas. Todos los miembros de la comunidad tienen una cuenta bancaria en el banco, y la empresa de software es la que se ha encargado del desarrollo de todos los sistemas".

De los grupos 5, 6 y 7 no se dirá nada, quedando así en el anonimato.

Será necesario disponer de ordenadores y de la creación de cuentas de correo electrónico para cada miembro de la clase, además deberá de tenerse acceso a Internet para poder acceder a las herramientas.

Sesión 3: ¿Cómo se juega?

Será la sesión preparatoria para el juego, cada grupo deberá investigar en Internet siguiendo las directrices que tenían en su ficha, y siempre con la ayuda del profesor para desarrollar las acciones que crean convenientes para la consecución de sus objetivos. La clase irá precedida por el siguiente vídeo:

https://www.youtube.com/watch?v=kgKyORdSim8

Acerca del uso de la herramienta Hacker Expirience. Que además el profesor se encargará de explicar.

Material

Será necesario que cada alumno cuente con un ordenador y que los componentes de los grupos se encuentren sentados de manera próxima, para poder desarrollar su trabajo de manera conjunta. Será necesario también disponer de cañón para proyectar el vídeo y las explicaciones del profesor, así como material que permita la reproducción multimedia.

Sesiones 4 y 5: Juguemos

Durante estas sesiones se desarrollará el juego. Cada uno siguiendo sus pautas, y a partir de toda su investigación desarrollada durante la sesión 3. El profesor actuará de orientador y de árbitro del juego, interviniendo en cualquier conflicto que pueda surgir. Los grupos deberán seguir los consejos que vaya ofreciendo el profesor, y según vaya desarrollándose, el profesor podrá informar a los grupos de lo que crea conveniente.

Durante estas tres sesiones, si lo estima conveniente introducirá nuevas tarjetas a determinados grupos para amenizar el desarrollo del juego y asemejarse con los cambios que a diario vivimos en nuestra vida.

Material

Se entregarán unas nuevas tarjetas que darán nuevas directrices (complementarias a las que originalmente se tenían) para los siguientes grupos:

Gobierno: Vais a sacar una ley controvertida y el representante deberá comunicarlo a la comunidad. Ley de Seguridad Cibernética: "Como tenéis serias sospechas de que se están cometiendo delitos, cualquier tipo de comunicación privada podrá ser espiada por la policía según su criterio".

Policía: Con la nueva ley, al principio la aprovecháis de manera eficaz, pero a medida que se desarrollan los acontecimientos la aprovecháis para invadir la intimidad de los demás, espiando conversaciones privadas que sabéis que no son constitutivas de delito.

Banco: Tenéis serias sospechas de que alguien en el banco está enviando información confidencial a un grupo de ciberdelincuentes, por lo que encargáis a uno de los responsables de seguridad del banco que espíe todas las conversaciones que se realizan desde el banco.

Empresa: Para reducir costes, echáis a uno de los responsables de seguridad, que se irá al grupo 5.

Ciberdelincuentes: Vais a establecer contacto con un trabajador del banco para intentar sobornarlo y que os facilite información confidencial del mismo. Además se ha unido a vosotros un trabajador de la empresa que intentará vengarse de ella a través del ataque a su seguridad.

Hacker: Descubres por una conversación privada que el grupo 5 es un grupo de ciberdelincuentes al que se acaba de unir un trabajador de la empresa por despecho. Tu harás lo posible por unirte a este grupo porque te sientes muy afín a la filosofía hacker.

Ciberladrones: No se establecen nuevas directrices.

Tabla 3. Fichas para repartir en el desarrollo del juego.[3]

[3] Las imágenes obtenidas para esta tabla están libres de copyright obtenidas de bancos de imágenes públicos

Sesiones 6, 7 y 8: Descubramos lo que hemos hecho

En esta sesión se concluirá el juego. Cada grupo deberá hacer una presentación de 10 – 15 minutos minutos en la que expliquen, cuál era su papel y sus objetivos dentro del juego así como las actuaciones que han llevado a cabo y las consecuencias que creen que han tenido, además de hacer un repaso a la investigación realizada al inicio.

Cada grupo habrá recibido en la sesión anterior una ficha que le indicará los puntos mínimos que deberá cubrir su presentación.

Al concluir cada presentación se abrirá un turno de preguntas de un máximo de 2 minutos al grupo por parte de cualquier miembro de la comunidad.

Material

Gobierno:

- Resumen de la legislación vigente en materia de ciberdelincuencia
- Políticas de seguridad de la información

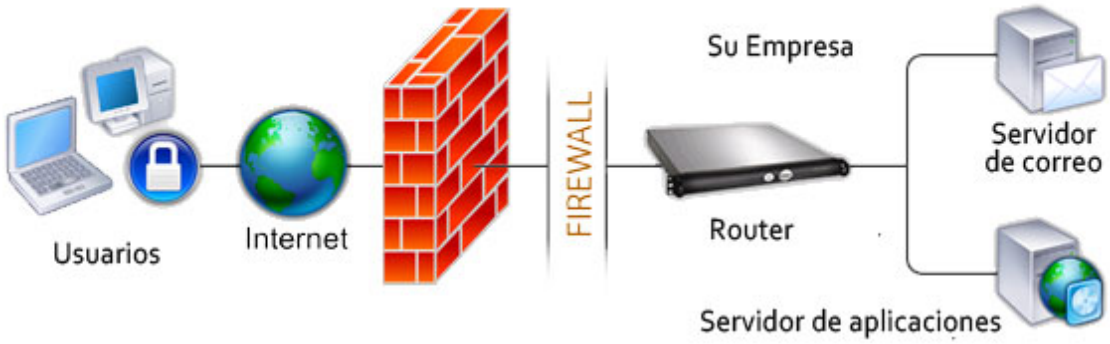
Policía:

- Herramientas de prevención de ataques
- Herramientas para detección de fraudes y delitos informáticos

Banco:

- Herramientas de prevención de ataques

- Herramientas de recuperación ante ataques o fallos de seguridad informática



Empresa:

- Herramientas de prevención de ataques
- Herramientas de recuperación ante ataques o fallos de seguridad informática

Ciberdelincuentes:

- Phishing
- Malware: Qué es y tipos de malware que existen
- DoS
- Ingeniería Social

Hacker:

- Malware: Qué es y tipos de malware que existen

Ciberladrones:

- Phishing
- Fraude electrónico
- Ingeniería social
- Cómo actuar para no dejar pistas.

Tabla 4. Puntos a incluir en las presentaciones.[4]

Sesión 9: ¿Cuáles son las consecuencias de nuestros actos?

Esta sesión va encaminada a debatir las consecuencias que han tenido cada uno de los actos que se han ido desarrollando en el juego. Los puntos a debatir serán propuestos por el propio alumnado, aunque como mínimo deberán cubrirse los siguientes puntos:

[4] Las imágenes obtenidas para esta tabla están libres de copyright obtenidas de bancos de imágenes públicos

- Consecuencias que tiene la legislación en materia de Internet en nuestras vidas
- Estamos dispuestos a perder el derecho a la intimidad a cambio de la seguridad
- ¿Es correcto realizar acciones legales pero no éticas si nos lo manda nuestro jefe?
- Consecuencias que puede tener no invertir el suficiente empeño en seguridad informática
- ¿Existen casos en los que el malware esté justificado ante algo que consideramos injusto?
- ¿Cómo podemos actuar para evitar ser defraudados?

Material

El material necesario para el desarrollo de esta actividad será un cañón para mostrar las imágenes y los vídeos que amenicen el debate. En concreto las siguientes fichas:

Figura 9. Consecuencias que tiene la legislación en materia de Internet en nuestras vidas

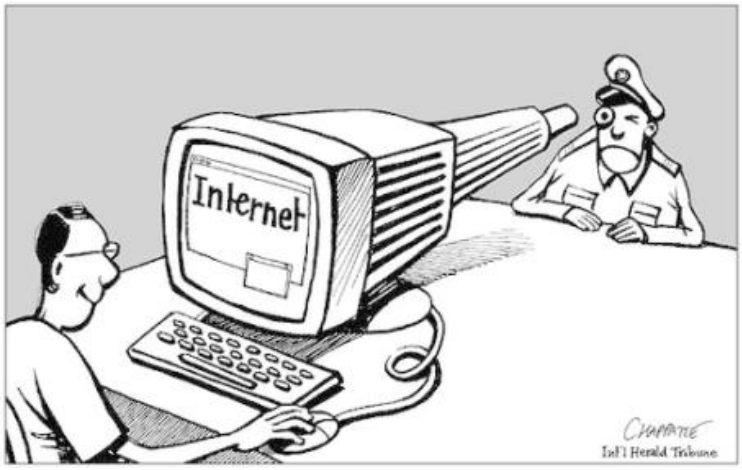


Figura 10. Estamos dispuestos a perder el derecho a la intimidad a cambio de la seguridad

Figura 11. ¿Es correcto realizar acciones legales pero no éticas si nos lo manda nuestro jefe?

Figura 12. Consecuencias que puede tener no invertir el suficiente empeño en seguridad informática

Figura 13. ¿Existen casos en los que el malware esté justificado ante algo que consideramos injusto?

Figura 14. ¿Cómo podemos actuar para evitar ser defraudados?

[5]

Sesión 10: Evaluación

Durante esta sesión se realizará una prueba escrita que vendrá detallada en el siguiente punto. Evaluación.

Criterios de evaluación de la asignatura

Según viene recogido en el BOE [2], los criterios de evaluación de la asignatura Informática de 4º de ESO.

[5] Las imágenes obtenidas para estas fichas están libres de copyright obtenidas de bancos de imágenes públicos

Instalar y configurar aplicaciones y desarrollar técnicas que permitan asegurar sistemas informáticos interconectados.

Se valora con este criterio la capacidad de localizar, descargar e instalar aplicaciones que prevengan el tráfico no autorizado en redes sobre diversos sistemas operativos. A su vez, se trata de identificar elementos o componentes de mensajes que permitan catalogarlos como falsos o fraudulentos, adoptar actitudes de protección pasiva, mediante la instalación y configuración de aplicaciones de filtrado y eliminación de correo basura, y de protección activa, evitando colaborar en la difusión de mensajes de este tipo.

Interconectar dispositivos móviles e inalámbricos o cableados para intercambiar información y datos.

Se pretende evaluar la capacidad de crear redes que permitan comunicarse a diferentes dispositivos fijos o móviles, utilizando todas sus funcionalidades e integrándolos en redes ya existentes. También se trata de conocer los distintos protocolos de comunicación y los sistemas de seguridad asociados, aplicando el más adecuado a cada tipo de situación o combinación de dispositivos.

Obtener imágenes fotográficas, aplicar técnicas de edición digital a las mismas y diferenciarlas de las imágenes generadas por ordenador.

Este criterio pretende valorar la capacidad de diferenciar las imágenes vectoriales de las imágenes de mapa de bits. Se centra en la captación de fotografías en formato digital y su almacenamiento y edición para modificar características de las imágenes tales como el formato, resolución, encuadre, luminosidad, equilibrio de color y efectos de composición.

Capturar, editar y montar fragmentos de vídeo con audio.

Los alumnos han de ser capaces de instalar y utilizar dispositivos externos que permitan la captura, gestión y almacenamiento de vídeo y audio. Se aplicarán las técnicas básicas para editar cualquier tipo de fuente sonora: locución, sonido ambiental o fragmentos musicales, así como las técnicas básicas de edición no lineal de vídeo para componer mensajes audiovisuales que integren las imágenes capturadas y las fuentes sonoras.

Diseñar y elaborar presentaciones destinadas a apoyar el discurso verbal en la exposición de ideas y proyectos.

Se pretende evaluar la capacidad de estructurar mensajes complejos con la finalidad de exponerlos públicamente, utilizando el ordenador como recurso en las presentaciones. Se valorará la correcta selección e integración de elementos

multimedia en consonancia con el contenido del mensaje, así como la corrección técnica del producto final y su valor discurso verbal.

Desarrollar contenidos para la red aplicando estándares de accesibilidad en la publicación de la información.

Se pretende que los alumnos utilicen aplicaciones específicas para crear y publicar sitios web, incorporando recursos multimedia, aplicando los estándares establecidos por los organismos internacionales, aplicando a sus producciones las recomendaciones de accesibilidad y valorando la importancia de la presencia en la Web para la difusión de todo tipo de iniciativas personales y grupales.

Participar activamente en redes sociales virtuales como emisores y receptores de información e iniciativas comunes.

Este criterio se centra en la localización en Internet de servicios que posibiliten la publicación de contenidos, utilizándolos para la creación de diarios o páginas personales o grupales, la suscripción a grupos relacionados con sus intereses y la participación activa en los mismos. Se valorará la adquisición de hábitos relacionados con el mantenimiento sistemático de la información publicada y la incorporación de nuevos recursos y servicios. En el ámbito de las redes virtuales se ha de ser capaz de acceder y manejar entornos de aprendizaje a distancia y búsqueda de empleo.

Identificar los modelos de distribución de «software» y contenidos y adoptar actitudes coherentes con los mismos.

Se trata de evaluar la capacidad para optar entre aplicaciones con funcionalidades similares cuando se necesite incorporarlas al sistema, teniendo en cuenta las particularidades de los diferentes modelos de distribución de «software». Se tendrá en cuenta el respeto a dichas particularidades y la actitud a la hora de utilizar y compartir las aplicaciones y los contenidos generados con las mismas. Asimismo, el respeto a los derechos de terceros en el intercambio de contenidos de producción ajena.

Contenidos - Criterios de evaluación – Indicadores del tema

Contenidos	Criterios de evaluación	Indicadores
Seguridad en Internet. El correo masivo y la protección frente a diferentes tipos de programas, documentos o mensajes susceptibles de causar perjuicios. Importancia de la adopción de medidas de seguridad activa y pasiva.	Desarrollar técnicas que permitan asegurar sistemas informáticos interconectados.	• Distingue los distintos tipos de amenazas que tiene un sistema informático • Clasifica los tipos de vulnerabilidades de un sistema • Conoce y clasifica los tipos de herramientas que le permiten prevenir ataques • Conoce y clasifica las herramientas que permiten subsanar las consecuencias de un ataque • Sabe establecer un sistema de seguridad de un sistema informático • Conoce como actuar ante el correo basura

Tabla 5. Contenidos, criterios de evaluación e indicadores

Instrumentos de evaluación

Parte	Teoría	Prácticas	
Porcentaje de cada parte	40%	60%	
Instrumento	Prueba escrita	Presentación	Desarrollo del proyecto
Porcentaje	100%	60%	40%

Tabla 6. Indicadores de evaluación

- General: Será necesario aprobar por separado tanto la parte de teoría como la parte de prácticas.
- Teoría:
  - Asistencia
    - Si se tienen faltas injustificadas se suspenderá la unidad
  - Prueba escrita:
    - Será imprescindible obtener al menos un 5 sobre 10 en la nota de esta prueba escrita, para poder aprobar la parte teórica de la asignatura
- Prácticas:
  - Desarrollo del proyecto:
    - Observación directa:
      - Se valorará la participación en el proyecto, la implicación y la autonomía de cada alumno así como su colaboración y trabajo en equipo. Según este criterio el profesor pondrá una nota máxima de 4 puntos.
  - Presentación:
    - Será obligatorio que todos los miembros participen en la presentación para aprobar.
    - Los aspectos a tener en cuenta para poner una nota máxima de 6 puntos en la presentación serán:
      - Se cubren todos los aspectos mínimos que se le ha propuesto al grupo
      - Calidad de la presentación.
      - Calidad del trabajo en equipo.
  - Asistencia:
    - Si se tienen faltas injustificadas se suspenderá la unidad

Recuperación: La parte de teoría tendrá una prueba escrita de recuperación una semana después a la ordinaria. Ese mismo día podrá realizarse la presentación quien no la haya hecho en la fecha asignada, con una penalización de un 10% en la nota final.

La prueba escrita para la evaluación de la parte teórica viene adjunta en el Anexo I

4.2. Medidas para atender al alumnado con necesidades específicas de apoyo educativo

Está claro que en la educación, como en el resto de la vida no existen dos personas iguales. Cada alumno y cada alumna tiene diferentes motivaciones, expectativas intereses, capacidades, ritmos de aprendizaje, etc. Este hecho exige que el profesorado plantee diferentes alternativas y opciones a cada uno según estos parámetros ofreciendo oportunidad de desarrollarse a todos y todas [29].

El planteamiento de la metodología hecho en esta unidad, facilita que cada alumno se implique en el trabajo según sus motivaciones y expectativas, aumentando el interés que mostrará en el desarrollo, y por supuesto facilitará la integración y la especialización en su desarrollo al alumnado con necesidades específicas de apoyo educativo.

4.3. Transversalidad

El proyecto desarrollado en esta unidad permite el tratamiento de los siguientes temas transversales:

El principal tema transversal a tratar será la ética informática. Las actividades y los debates realizados en la metodología permitirán analizar uno a uno todas los actos que se han realizado con lo que se pretende que el alumnado recoja una actitud crítica y sepa distinguir entre la legalidad y la ética de sus actos.

Además por su naturaleza, permitirá mejorar las habilidades sociales y el trabajo en equipo y el respeto a los compañeros, si se realizan de manera correcta.

4.4. Innovación

Por tratar tan de cerca el tema de la ética informática, estamos trabajando la educación en valores del alumnado.

La metodología por proyectos es altamente innovadora y permite convertir al alumnado en actor principal del proceso de aprendizaje y no en un mero receptor pasivo de la información.

El uso de herramientas altamente innovadoras utilizadas en el proyecto permite trabajar y fomentar el manejo de las herramientas TIC.

Se incitará al alumnado a realizar exposiciones que fomentarán su mejora en la habilidad de expresión oral.

Por otro lado el proyecto permitirá simular situaciones reales de la vida y que propiciará un debate en el que estudien las consecuencias que tienen sobre los demás sus actos. Este hecho hace que aprendan a trabajar la convivencia con los demás.

Se fomentará además el trabajo y la investigación para el desarrollo de sus actividades, a través de bibliotecas (tanto físicas como digitales).

5. Bibliografía

[1] Carmen, E. D. (2014). *Plan de Centro.* Jaén, España: IES Virgen del Carmen.

[2] Ministerio de Educación y Ciencia. (2007). *REAL DECRETO 1631/2006, de 29 de diciem- bre, por el que se establecen las enseñanzas mínimas correspondientes a la Educación Secundaria Obligatoria.* Madrid: Gobierno de España.

[3] DeLooze, L.L. (2004). Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC

[4] Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. In The economics of information security and privacy (pp. 265-300). Springer Berlin Heidelberg.

[5] Yar, M. (2013). Cybercrime and society. Sage.

[6] IEEE. (1 de Enero de 2014). *IEEE Cloud Computing Vulnerabilities*. Retrieved 16 de Junio de 2015 from IEEE Cloud Computing Vulnerabilities: http://www.infoq.com/articles/ieee-cloud-computing-vulnerabilities

[7] Symantec Corporation. (2008). *Symantec Internet Security Threat Report.* Cupertino: Symantec Corporation.

[8] "An Undirected Attack Against Critical Infrastructure". United States Computer Emergency Readiness Team(us-cert.gov). [Recurso web accedido el 16 de junio de 2015].

[9] Aycock, J. (2006). *Computer Viruses and Malware*. Springer.

[10] Core One Information Technology (2014). Tipos de ataques informáticos. [Recurso web accedido el 16 de junio de 2015].

[11] Wysopal, C., & Eng, C. (2007). Static detection of application backdoors. Black Hat.

[12] Desnos, A., Filiol, É., & Lefou, I. (2011). Detecting (and creating!) a HVM rootkit (aka BluePill-like). Journal in computer virology, 7(1), 23-49.

[13] Landwehr, C. E; A. R Bull; J. P McDermott; W. S Choi (1993). A taxonomy of computer program security flaws, with examples.

[14] Ramneek, P. (2003). Bots &; Botnet: An Overview. SANS Institute.

[15] Sánchez Rojo, E. (2003). Adware. PC Actual. Personal computer, (157), 254-260.

[16] Núñez, E. V. (2007). Fraudes informáticos en red: del phishing al pharming. La ley penal: revista de derecho penal, procesal y penitenciario, (37), 57-66.

[17] AV-Test. (14 de enero de 2015). Malware Statistics & Trends Report. Retrieved 16 de junio de 2015 en AV-Test: http://www.av-test.org/en/statistics/malware/

[18] G Data SecurtyLabs. (20 de diciembre de 2014). New Malware Strains Recorded During Second Half of 2014 More Than Double in Volume. Retrieved 16 de junio de 2015 from EnigmaSoftware: http://www.enigmasoftware.com/malware-strains-recorded-h2-2014-more-than-double-volume/

[19] elpais.es/agencias. (2006). El Congreso aprueba definitivamente la LOE con la oposición del PP. *El País*. http://sociedad.elpais.com/sociedad/2006/04/06/actualidad/1144274403_850215.html

[20] Verizon. (1 de enero de 2015). Verizon Data Breach Report 2015: Top 10 Charts and Summary. Retrieved 16 de junio de 2015 from Calyptix Security: http://www.calyptix.com/research-2/verizon-data-breach-report-2015-top-10-charts-and-summary/

[21] Henry, A. (21 de diciembre de 2013). *The Difference Between Antivirus and Anti-Malware (and Which to Use)*. Retrieved 16 de junio de 2015 from lifehacker: http://lifehacker.com/the-difference-between-antivirus-and-anti-malware-and-1176942277

[22] Oppliger, R. (1997). Internet security: firewalls and beyond. Communications of the ACM, 40(5), 92-102.

[23] Hassan, T. (2006). Towards eradication of SPAM: A study on intelligent adaptive SPAM filters (Doctoral dissertation, Murdoch University).

[24] Gómez, J. (2006). Copias de seguridad. Todo linux: la revista mensual para entusiastas de GNU/LINUX, (63), 42-46.

[25] Clarke, E. M., & Wing, J. M. (1996). Formal methods: State of the art and future directions. ACM Computing Surveys (CSUR), 28(4), 626-643.

[26] Carlin, S., & Curran, K. (2011). Cloud computing security.

[27] Dropbox. (1 de junio de 2015). ¿Hasta qué punto es seguro Dropbox? Retrieved 16 de junio de 2015 from Dropbox: https://www.dropbox.com/help/27

[28] ARANDA, S. R., & SECUNDARIA, E. S. APRENDIZAJE BASADO EN PROYECTOS.

[29] Gil, F. G. (2011). Inclusión y atención al alumnado con necesidades educativas especiales en España. Participación educativa, (18), 60-78.

Anexo I

Prueba escrita

Esta será la prueba escrita que el alumnado tendrá que superar para aprobar la parte teórica:

Parte I (7,5 puntos)

1. Enumera los distintos tipos malware que conoces (1,5 punto)

2. ¿Cómo podrías prevenir que en tu casa alguien pudiera caer en el fraude denominado "Phising"? (1,5 punto)

3. ¿Cuáles son las diferencias entre las herramientas preventivas y las herramientas paliativas? (1,5 punto)

4. ¿Cuáles son las ventajas de utilizar una buena política de seguridad en un sistema informático? (1,5 punto)

5. ¿Qué diferencia hay entre virus y malware? (1,5 punto)

Parte II (2,5 puntos)

Sólo hay una respuesta válida, cada 3 respuestas incorrectas, restará (0,5 puntos).

6. A la hora de establecer una contraseña segura, debes de tener en cuenta (0,5 puntos):

1) Que sea fácil de recordar
2) Que tenga letras y números solamente
3) Que sea diferente en todas tus cuentas importantes
4) Que sea siempre *1234*

7. Cuál de las siguientes es una buena estrategia de seguridad (0,5 puntos):

1) Guardar tus contraseñas en un archivo de texto en tu escritorio
2) Cambiar tu contraseña frecuentemente
3) Mantener una misma contraseña en todas tus cuentas importantes
4) No establecer una contraseña en tu cuenta de usuario del S.O.

8. En un ataque por fuerza bruta (0,5 puntos)

1) Las contraseñas que sólo tienen dígitos son más fáciles de descifrar
2) La contraseña *abc1234* es la más segura
3) La longitud de la contraseña no influye en su vulnerabilidad
4) Todas las respuestas anteriores son falsas

9. Al recibir un correo electrónico, ¿Cuál es la mejor actitud a tomar? (0,5 puntos)

1) Enviar los datos de nuestra tarjeta si nos lo piden
2) Verificar la autenticidad del emisor del correo
3) Las dos respuestas anteriores son verdaderas
4) No abrir nunca ningún correo que no estemos esperando

10. Si recibes un correo electrónico con un enlace a una web, ¿Qué actitud es la más apropiada?

1) Abrir el enlace, por si es algo importante
2) No abrir en ningún caso el enlace
3) Verificar la autenticidad del mensaje, y analizar que no tenga virus antes de abrirlo

Todas las respuestas anteriores son falsas