UNIVERSIDAD DE BURGOS

MÁSTER UNIVERSITARIO EN PROFESOR DE EDUCACIÓN SECUNDARIA OBLIGATORIA Y BACHILLERATO, FORMACIÓN PROFESIONAL Y ENSEÑANZA DE IDIOMAS

TRABAJO FIN DE MÁSTER. CURSO 2017- 2018

Formación sobre el uso seguro y responsable de Internet para alumnos de formación profesional

Cristina de la Peña Acero

Especialidad: Tecnología Industrial

Tutor: David Hermindo Martín Alonso

Facultad de Educación

Contenido

1. Resumen/Abstract

En un contexto socioeconómico en el que la ciberseguridad cobra cada día más importancia, el presente trabajo tiene como fin cuestionarse el papel que el sistema educativo, y sobre todo la formación profesional, está jugando en la educación de los alumnos en el uso seguro y responsable de las TIC, cuyo uso es hoy en día imprescindible en cualquier sector laboral.

La primera parte del trabajo se centra en justificar por qué se considera necesario reforzar los conocimientos que pueden tener los alumnos de los ciclos de FP en materia de *ciberseguridad*, mientras que en la segunda se proponen una serie de actividades sencillas para que estos puedan reforzar las destrezas básicas que los capaciten para el uso seguro y responsable de las nuevas tecnologías en su futuro puesto de trabajo.

In the actual socio-economical context where cybersecurity plays every day a more important role, the present work pretends to study the role that the Spanish educational system, and about all the Professional Training, are playing in the training of the students in the use secure and responsible of the ICT, which are nowadays essential in all the professional sectors.

The first part of the work consists in answering the question why is necessary to reinforce the knowledge that the students of the professional training may have regarding cybersecurity, while in the second part we propose some simple activities to work the basic skills related to the use secure and responsible of the new technologies in their future job.

1.2 Palabras Clave/ Key words

Formación Profesional, TIC, seguridad, Internet, tecnologías de la información, competencia digital, seguridad digital, uso seguro y responsable, ciberseguridad.

Professional Training, ICT, security, Internet, information technologies, digital competence, digital security, use secure and responsible, cybersecurity,

2. Introducción

La nueva sociedad de la información, con Internet a la cabeza, ha creado un nuevo horizonte en la concepción de la comunicación, la economía, las relaciones interpersonales y también en la propia enseñanza.

El sector laboral es uno de los entornos donde más ha impactado esta transformación ya que gracias a las nuevas tecnologías han cambiado radicalmente tanto la naturaleza de la producción como su organización (Elboj, 1998). Las formas de producción y las condiciones del trabajo han evolucionado con rapidez obligando a todos los estamentos de la sociedad a adaptarse a las nuevas circunstancias adquiriendo, bajo amenaza de exclusión del mercado laboral, los nuevos conocimientos y destrezas que nos permitan desenvolvernos con éxito en la nueva sociedad emergente.

Mientras que en la antigua sociedad industrial se priorizaba lo material considerando que los recursos materiales favorecían el éxito o el fracaso de países o personas, en la actual sociedad de la información no solo se prioriza el dominio de los recursos materiales sino también la capacidad intelectual, y sobre todo la selección y el procesamiento de la información como factores clave del éxito en todos los sentidos (Cabero, 2007).

Por su parte el mundo educativo no es ni mucho menos ajeno a toda esta revolución con la irrupción en las aulas de las famosas TIC. Sin embargo los experto alertan que la educación en la sociedad de la información no debe entenderse solo como formación en su uso, sino que **las TIC deben de saber utilizarse para desarrollar nuevas formas de enseñar y aprender**, mejorando así cada día más nuestra educación. Ello incluye, por lo tanto, las citadas habilidades para seleccionar de manera crítica la información para luego adecuarla al contexto y desarrollar así un nuevo conocimiento a partir de ella (Fernández, 2017).

De entre todas las etapas educativas, en los ciclos de formación profesional es sin duda donde más se debería tener garantías de que el alumnado posee las habilidades básicas necesarias que le capaciten para el buen uso y manejo de las tecnologías de la información. Ello es debido al perfil pre-profesional de su alumnado, que ya dentro de su propia formación incluye extensos periodos de prácticas en la propia empresa (lo que se denomina comúnmente como FCTs o Formación en el Centro de Trabajo) y aún más con la entrada en vigor de la FP Dual que permite realizar gran parte del proceso de formación dentro de la propia empresa.

Nos encontramos entonces aquí en un punto en el que mercado laboral y sector educativo convergen al coincidir en la necesidad de educar una nueva generación de individuos que sepan maximizar las potencialidades que todo el universo internet ofrece integrándolas en profundidad en su saber hacer cotidiano y laboral.

¿Pero está verdaderamente nuestro sistema educativo, y en especial el profesorado de FP preparado para asumir dicha responsabilidad? A sabiendas de que la implantación de las TIC es una realidad en casi la totalidad de los centros en nuestro país **¿estamos verdaderamente educando al alumnado en su uso productivo y sobre todo seguro y responsable?**

Según señalan numerosos expertos que estudian desde hace años el fenómeno, en la Educación Secundaria Obligatoria o ESO esta labor sigue recayendo en buena medida en el núcleo familiar, convirtiendo en muchos casos el uso y manejo de las TIC en una cuestión directamente vinculada a la clase social de los alumnos, generando por consiguiente desigualdades sociales dentro de las propias aulas.

El presente trabajo, parte de la hipótesis inicial de que a pesar de que la nueva sociedad de la información es ya una realidad en nuestro sistema educativo, **en la práctica no existe ninguna garantía de que el alumnado este adquiriendo las habilidades y competencias necesarias para su uso responsable, seguro y productivo** y que por ello existen claras desigualdades en ese campo entre los estudiantes en función del contexto socio-económico del centro educativo y de las familias.

Como consecuencia de ello, los estudiantes que acceden a los ciclos de Formación Profesional en cualquiera de sus modalidades (Básica, Media y Superior) en muchos casos están carentes de unas nociones básicas de seguridad en el uso de los dispositivos informáticos que a bien seguro deberán utilizar en el desempeño de sus futuros oficios sea cual sea su familia profesional.

Para poder verificar esta hipótesis, procederemos en primer lugar a realizar un análisis de la actual ley de educación y del papel que desempeñan las TIC en ella y en los currículos de las materias afines a las mismas. De confirmarse nuestras sospechas, pasaremos a continuación a diseñar una serie de actividades que complementen la formación de los estudiantes de formación profesional y así garantizar su acceso en óptimas condiciones a las FCTs y posteriormente al mundo laboral. .

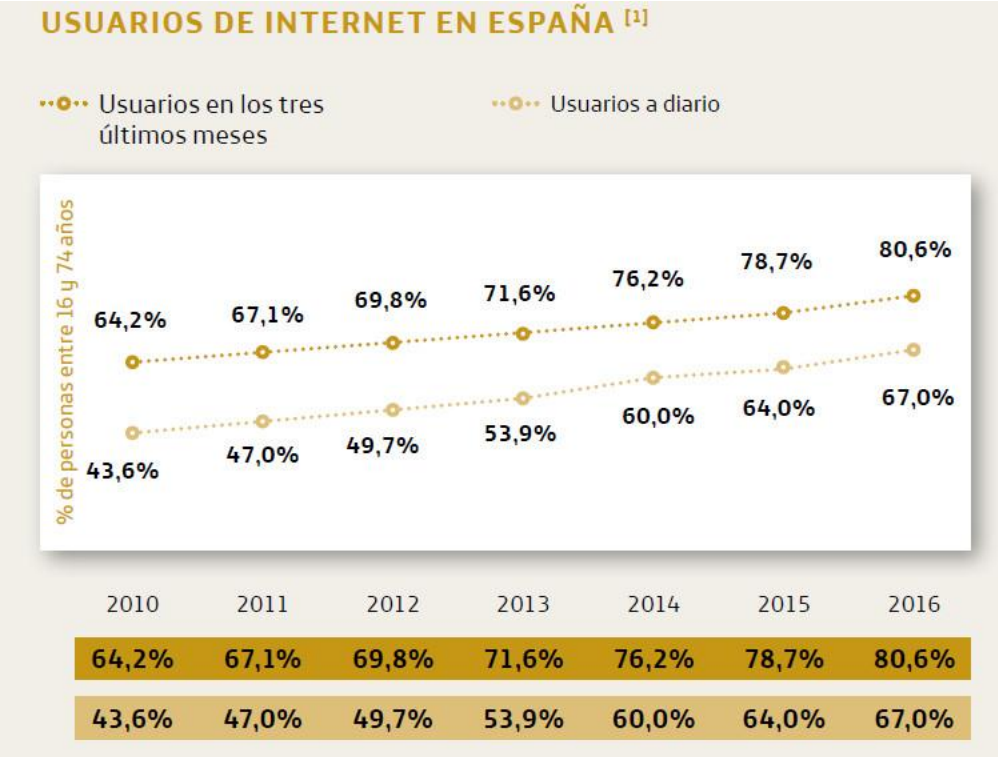
3. Contexto: la sociedad de la información en España.

Los informes de la Sociedad de la Información en España promovidos por Fundación Telefónica son publicaciones de referencia que anualmente muestra la situación, los avances y el uso en España de las comunicaciones y los servicios digitales. Las dos últimas ediciones, la décimo séptima y la décimo octava presentan de forma objetiva la situación de España en el despliegue de redes y en el uso y consumo de las nuevas tecnologías de la comunicación.

Con el fin de contextualizar el presente trabajo en un marco general a nivel nacional, los siguientes apartados constituyen un resumen de aquellas partes del informe que resultan más interesante en nuestro caso, es decir, en todo lo relativo al uso de las TIC entre los jóvenes y el sector de la educación.

Datos de conectividad, acceso y terminales:

Ocho de cada diez españoles entre los dieciséis y los setenta y cuatro años ha usado Internet en los últimos tres meses durante el año 2016. De los más de 27,7 millones de usuarios de Internet en los que se traducen estas cifras, el 95 % es usuario frecuente, es decir, esos internautas acceden al menos a Internet una vez a la semana lo que supone un 76,5 % de la población total. Por su parte el número de usuarios intensivos, aquellos que acceden diariamente, supone ya el 82,9 % de los usuarios de Internet hasta los 23 millones de internautas.

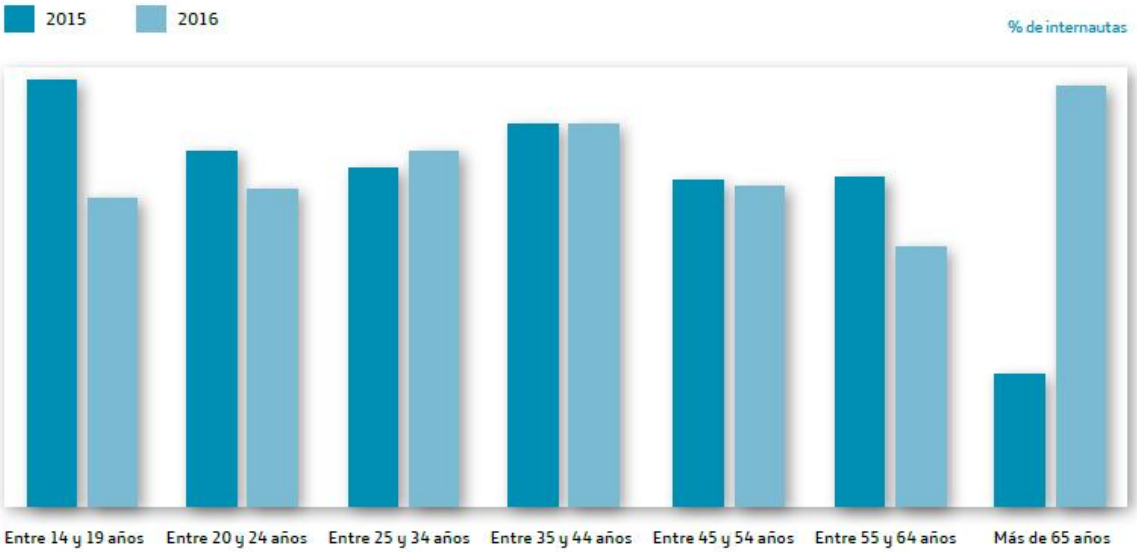


	2010	2011	2012	2013	2014	2015	2016
	64,2%	67,1%	69,8%	71,6%	76,2%	78,7%	80,6%
	43,6%	47,0%	49,7%	53,9%	60,0%	64,0%	67,0%

1. **Evolución del nº de usuarios de Internet en España**

Dos de los factores principales que influyen a la hora de acceder a Internet son la edad y el nivel de estudios. La edad es la variable que más condiciona el uso de Internet en nuestro país, ya que la práctica totalidad de los jóvenes de edades comprendidas entre los dieciséis y los veinticuatro años ha accedido a Internet en los últimos tres meses (el 98,4 %), mientras que esta cifra es del 34,7 % de las personas de edades comprendidas entre los sesenta y cinco y los setenta y cuatro años.

FIGURA 17. UTILIZACIÓN DE LA *TABLET* POR PARTE DE LOS INTERNAUTAS DE CADA SEGMENTO



	Entre 14 y 19 años	Entre 20 y 24 años	Entre 25 y 34 años	Entre 35 y 44 años	Entre 45 y 54 años	Entre 55 y 64 años	Más de 65 años
2015	42,5%	35,4%	34,0%	38,3%	32,6%	33,1%	13,2%
2016	30,9%	31,9%	35,4%	38,5%	32,2%	26,2%	42,1%

Fuente: Telefónica. Datos de junio de 2016.

2. Evolución en el uso de la *Tablet* por segmentos de edad.

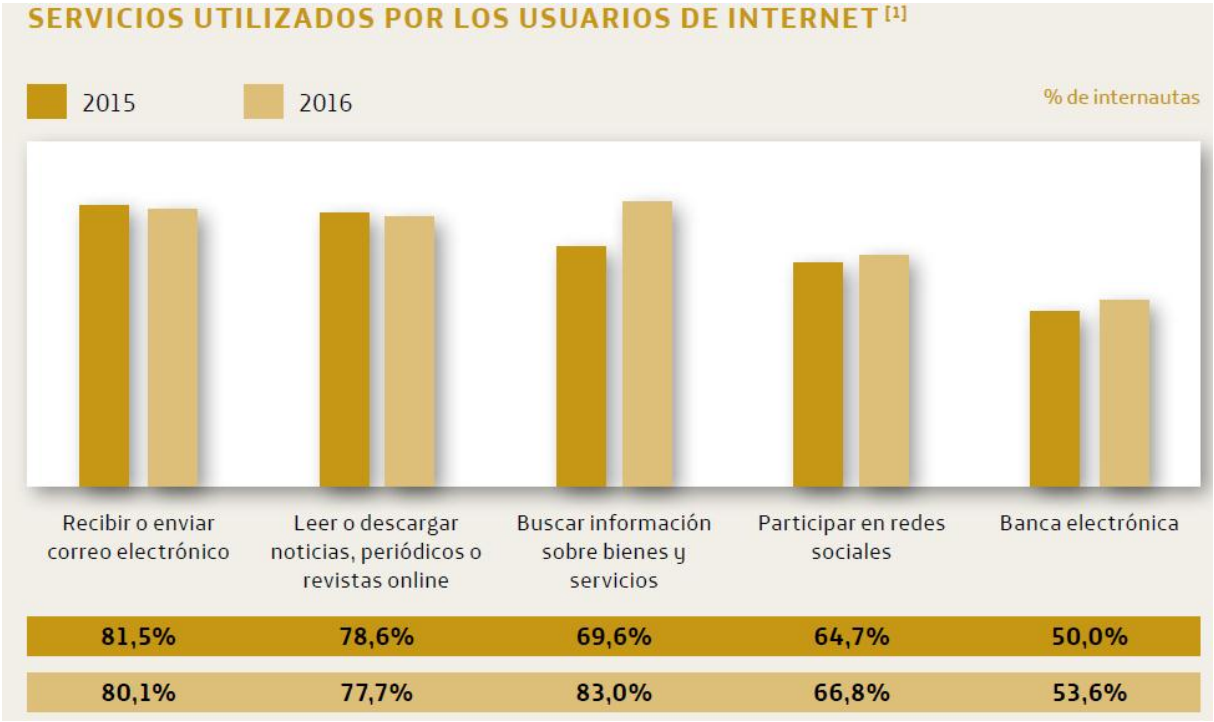
Por otro lado, si atendemos al nivel de estudios, se observa que el número de internautas pasa del 40,8 % entre las personas que solo han finalizado la educación primaria, hasta el 97,8 % en el caso de aquellos con estudios superiores. Esta diferencia es también importante entre los usuarios intensivos, aquellos que se conectan a Internet diariamente, ya que son el 63 % de los internautas que han finalizado la educación primaria y el 95,4 % de los internautas con estudios de licenciatura o máster terminado, hasta alcanzar el 97,5 % si los estudios terminados son de doctorado.

Respecto al género, no existen apenas diferencias en cuanto al uso de Internet entre los distintos sexos en España, con la excepción de la franja de edad comprendida entre los sesenta y cinco y los setenta y cuatro años.

Por su parte el teléfono móvil es el dispositivo utilizado mayoritariamente para acceder a Internet, pues así procede el 93,3 % de los internautas, 8,5 puntos porcentuales más que en el año 2015. Entre los jóvenes de edades comprendidas entre los dieciséis y los veinticuatro años el porcentaje es del 98,8 %.

Actualmente, el motivo más frecuente para acceder a la Red entre los internautas españoles es la búsqueda de información sobre productos y servicios, una de las actividades

que más crece en 2016. El 82,6 % de los usuarios de Internet accede con esa intención a la Red en 2016, frente al 69,6 % que lo hacía en 2015, 13 puntos porcentuales más. La segunda actividad más frecuente en 2016 ha sido la utilización del correo electrónico, un 80,1 %, aunque cada año va perdiendo relevancia y este año ha bajado 1,4 puntos. La tercera actividad es la lectura de noticias, periódicos o revistas online, con un 77,6 %, 0,9 puntos menos que en 2015.



3. **Servicios más utilizados por los internautas.**

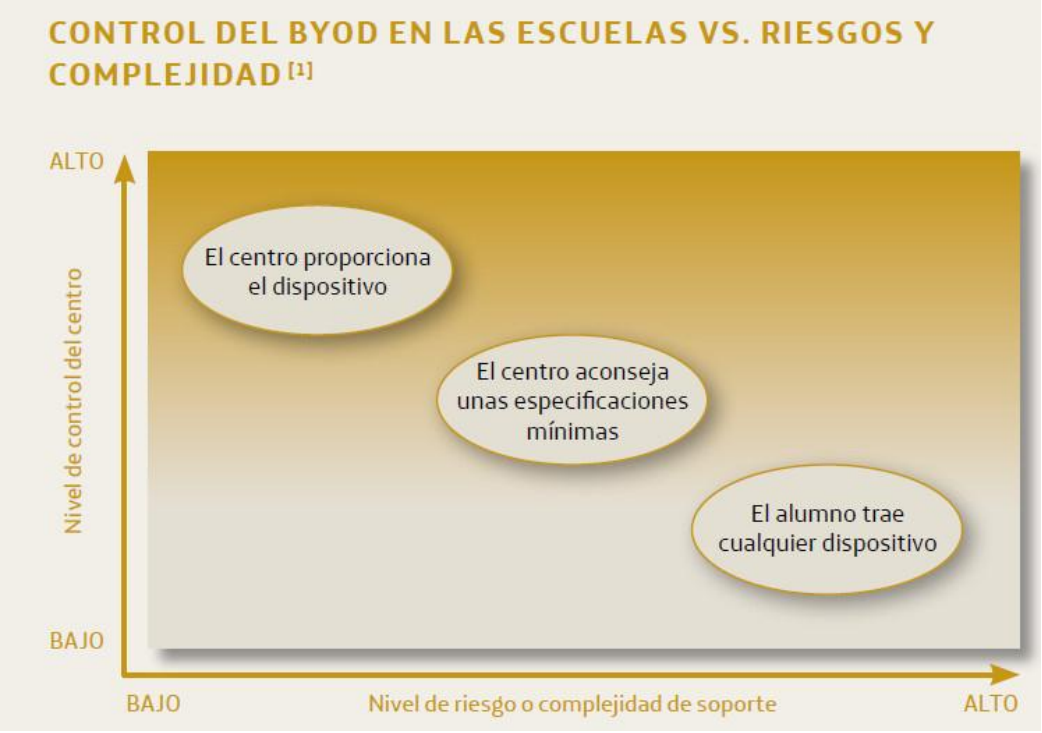
Los jóvenes de edades comprendidas entre los dieciséis y los veinticuatro años se decantan claramente por dos actividades principales: ver vídeos de sitios para compartir, como YouTube (92,5 %), que es ya la primera actividad en esta franja de edad, y participar en redes sociales (91,1 %).

TIC y educación: BYOD en las aulas y el video como elemento favorito:

El proceso educativo se enfrenta a retos muy estimulantes de cara a la preparación de las futuras generaciones para desenvolverse en un mundo cada vez más globalizado, en el que los cambios se suceden a gran velocidad y en el que la innovación es, quizá, la clave más importante del éxito, tanto profesional como personal. En este contexto, las tecnologías de la información y de las comunicaciones juegan un papel destacado, convirtiéndose en herramientas necesarias para abordar los desafíos educativos.

Uno de los desafíos actuales es desarrollar metodologías capaces de conjugar los procesos educativos tradicionales (basados en contenidos «analógicos») con los estudiantes nativos digitales, acostumbrados al acceso a la información y al entretenimiento a través de dispositivos electrónicos. En este sentido, la principal tendencia apunta hacia el uso de un dispositivo por alumno. Los centros educativos están incrementando la disponibilidad de estos dispositivos, aunque la inversión necesaria para lograr que todos los alumnos dispongan de ellos es elevada, sobre todo en un entorno de restricciones presupuestarias públicas.

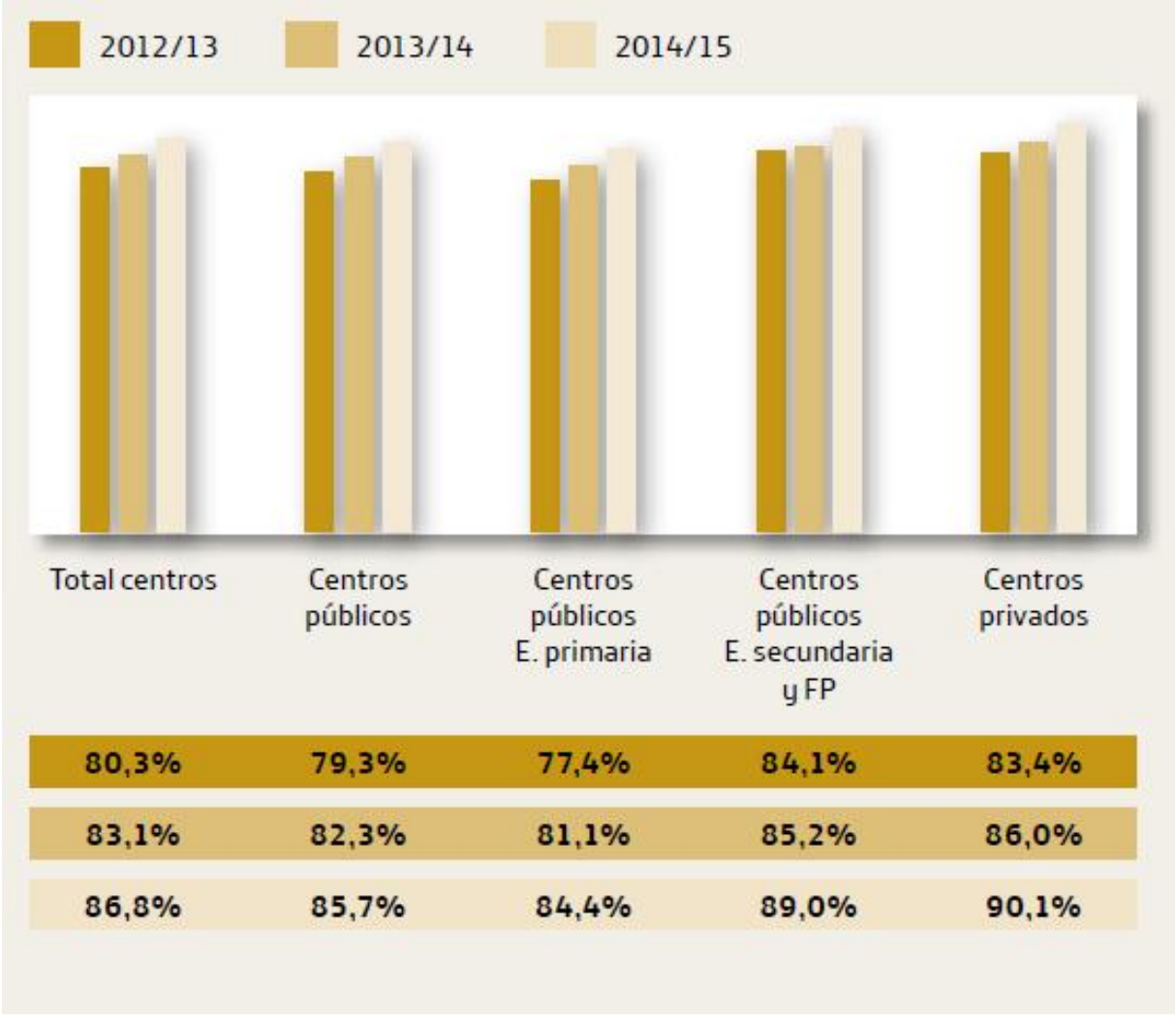
Ante esta situación, la solución planteada es la traslación del concepto BYOD (Bring Your Own Device) del ámbito empresarial al educativo, de forma que sean los alumnos quienes lleven sus propios dispositivos al aula. Sin embargo, aspectos como la igualdad entre los alumnos —podrían disponer de mejores dispositivos en función de la capacidad adquisitiva de sus familias—, la compatibilidad con los recursos educativos —pueden estar únicamente desarrollados para un sistema operativo—y sobre todo la seguridad y el mantenimiento de los mismos juegan en contra de esta tendencia.



4. El BYOD en las escuelas.

Uno de los factores de éxito de la introducción de los dispositivos en el aula (bien proporcionados por el centro educativo o bien mediante el BYOD) es contar con una conexión inalámbrica que permita el acceso de todos los alumnos. El número de centros

educativos que cuentan con conexión wifi en España creció casi 4 puntos porcentuales en 2015, situándose en el 86,8 %. En la educación secundaria, donde comienza a ser más habitual el BYOD, la conectividad wifi está presente en el 89 % de los centros. El mayor problema con el que cuentan los centros educativos en España para hacer frente a la utilización de un dispositivo por alumno es el bajo ancho de banda del que disponen ya que por ejemplo en el curso 2014-2015, solo el 25,6 % de los centros educativos contaba con conexión de más de 20 Mb/s. A pesar de este bajo porcentaje, la situación ha mejorado notablemente respecto al año anterior, cuando únicamente el 12 % disponía de conexión de más de 20 Mb/s.

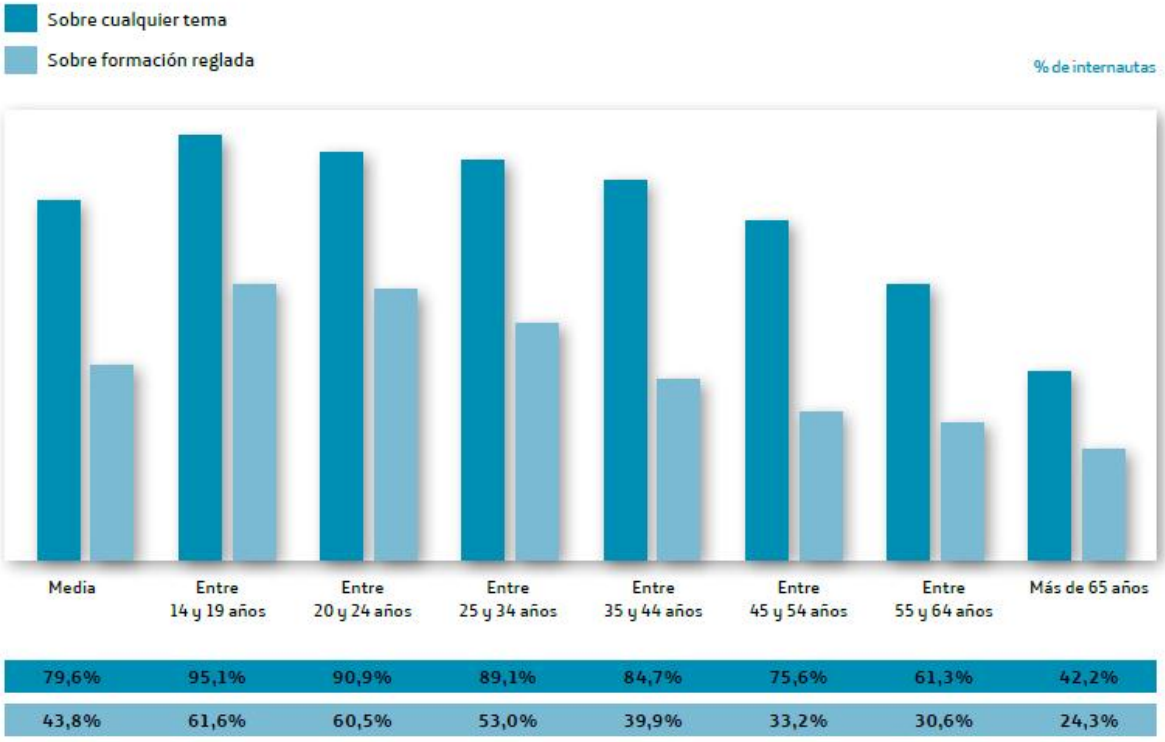


5. **Datos de conexión wifi en los centros educativos en los últimos años.**

Por su parte el vídeo se ha convertido también en un formato fundamental a la hora de realizar actividades formativas, hasta el punto de que el 95,1 % de los jóvenes de edades comprendidas entre los catorce y los diecinueve años utiliza Internet para acceder a vídeos

con carácter formativo y el 61,6 % para acceder a vídeos en el entorno de la educación reglada.

FIGURA 20. UTILIZACIÓN DE INTERNET PARA ACCEDER A VÍDEOS CON CARÁCTER FORMATIVO



6. Utilización de internet para acceder a vídeos con carácter educativo por segmentos de edad.

Más concretamente, la evolución muestra que el ocio es la primera motivación para muchos jóvenes para iniciarse en Internet, pero que posteriormente, con el paso del tiempo, descubren que Internet puede jugar un papel fundamental en su formación y pasa a ser este su principal interés en su uso.

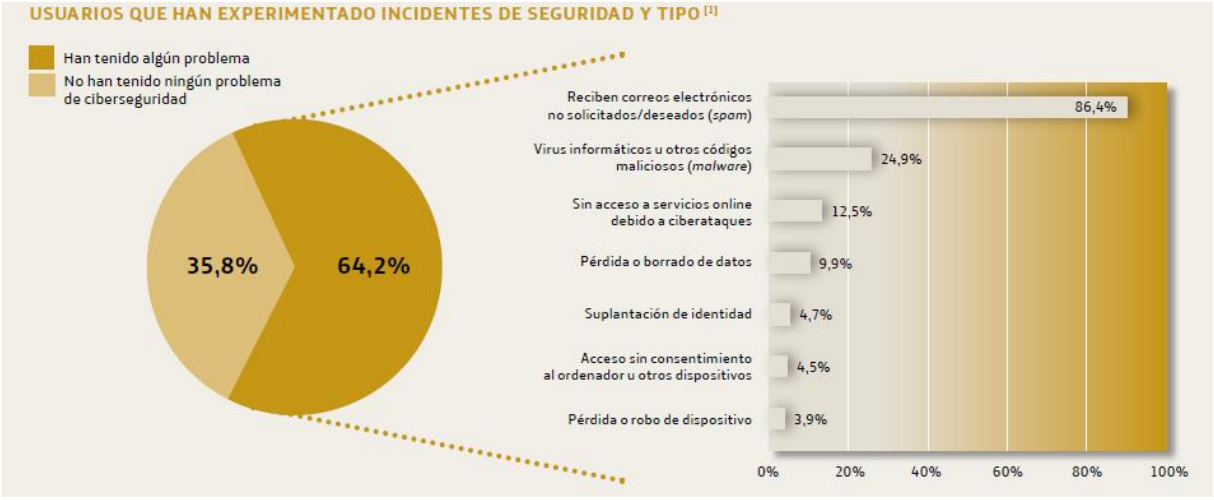
Ciberseguridad: más ciberataques y menos concienciación de los usuarios

En 2017 la ciberseguridad ha sido uno de los temas tecnológicos que más interés ha despertado en el mundo entero (Sociedad Digital España, 2017). Diferentes ataques masivos públicos que se han conocido durante este año han puesto de manifiesto la vulnerabilidad de algunos sistemas de información y han puesto de manifiesto en los medios de comunicación los riesgos generales de un uso indebido de la tecnología.

En 2016, el Foro Económico Mundial situó los ciberataques entre los riesgos con mayor probabilidad de ocurrencia, al mismo nivel que el desempleo o la inestabilidad social y por

encima incluso del terrorismo, lo que nos puede dar una idea de lo preocupante de la situación.

En España, el 64,2 % de los usuarios individuales declaran haber tenido alguna incidencia de seguridad. La más común, con mucha diferencia respecto al resto, es el spam (86,4 % de usuarios particulares), seguido del malware (24,9 %) y denegación de servicio (12,5 %). Estos porcentajes, declarados por los propios usuarios, contrastan muy significativamente con los datos arrojados por el escaneo real de los dispositivos que **elevan el porcentaje real de dispositivos infectados hasta el 63,9 %,** lo que nos da una idea de hasta qué punto el usuario es ingenuo en sus consideraciones de seguridad.



7. **Principales problemas de seguridad que han experimentado los usuarios.**

En relación a las medidas preventivas que los usuarios llevan a cabo para evitar los ataques o reducir su impacto, en el segundo semestre de 2016 destaca el uso de programas antivirus (72 %), las actualizaciones del sistema operativo (55,5 %) y el uso de cortafuegos (39,6 %). Entre las medidas de seguridad activas, las más comunes son el uso de contraseñas (55,7 %), eliminación de archivos temporales y cookies (43,6 %) y las copias de seguridad de archivos (33,6 %). Y lo que es relevante de estos datos es que todos ellos disminuyeron con respecto al año 2015. **Es decir, cada vez los usuarios se preocupan menos por laprotección de sus equipos.**

8. Principales medidas de seguridad adoptadas por los usuarios.

A diferencia de los usuarios individuales, **la concienciación de las empresas respecto al impacto de los incidentes ha crecido**. Así, según un estudio de la compañía de seguros Zurich, en 2015 el 25,5 % de las pequeñas y medianas empresas pensaba que no eran relevantes para los cibercriminales, mientras que en 2016 el porcentaje se redujo al 19,5 %, indicando una creciente por parte de las PYMES de ser objetivo de algún ataque que pudiera perjudicar su operativa e incluso ocasionar la desaparición de la misma.

En este escenario, el sector de la ciberseguridad se sitúa como uno de los más dinámicos ligados a la economía y sociedad digitales hasta el punto que esta se está convirtiendo en un activo estratégico prioritario en las políticas de seguridad nacional de los Estados.

9. Gasto estimado en ciberseguridad en Europa en los últimos años.

4. La competencia digital en la LOMCE

4.1 Objetivos que persigue la LOMCE

Según la ley Orgánica 8/2013, de 9 de diciembre, para la mejora de la calidad educativa, una lectura detallada de sus disposiciones generales nos dice que los **objetivos que persigue la nueva ley** de educación son los siguientes:

- Reducir la tasa de abandono temprano de la educación
- Mejorar los resultados educativos de acuerdo a los criterios internacionales
- Mejorar la empleabilidad y el espíritu emprendedor de los estudiantes
- El aumento de la autonomía de los centros
- **Fomentar el uso generalizado de las Tecnologías de la Información y la Comunicación**
- El fomento de plurilingüismo
- Modernización de la Formación Profesional

Concretamente en el apartado XI de dichas disposiciones se nos dice:

"Las Tecnologías de la Información y la Comunicación serán una pieza fundamental para producir el ***cambio metodológico*** *que lleve a conseguir el objetivo de mejora de la calidad educativa. Asimismo****, el uso responsable y ordenado de estas nuevas tecnologías por parte de los alumnos y alumnas debe estar presente en todo el sistema educativo****."*

Y continúa:

"Las Tecnologías de la Información y la Comunicación serán también una ***herramienta clave en la formación del profesorado y en el aprendizaje de los ciudadanos a lo largo de la vida****, al permitirles compatibilizar la formación con las obligaciones personales o laborales y, asimismo, lo serán en la gestión de los procesos."*

Las competencias clave:

Según la LOMCE las orientaciones de la Unión Europea insisten en la necesidad de la adquisición de las **competencias clave** por parte de la ciudadanía como condición indispensable para lograr que los individuos alcancen un pleno desarrollo personal, social y profesional que se ajuste a las demandas de un mundo globalizado y haga posible el desarrollo económico, vinculado al conocimiento.

Las competencias, por tanto, se conceptualizan como un "saber hacer" que se aplica a una diversidad de contextos académicos, sociales y profesionales. Para que la transferencia a distintos contextos sea posible resulta indispensable una comprensión del conocimiento presente en las competencias y la vinculación de este con las habilidades prácticas o destrezas que las integran.

El aprendizaje basado en competencias se caracteriza por su **transversalidad, su dinamismo y su carácter integral, el proceso de enseñanza-aprendizaje competencial debe abordarse desde todas las áreas de conocimiento** y por parte de las diversas instancias que conforman la comunidad educativa, tanto en los ámbitos formales como en los no formales e informales. Su dinamismo se refleja en que las competencias implican un proceso de desarrollo mediante el **cual los individuos van adquiriendo mayores niveles de desempeño en el uso de las mismas conforme pasa el** tiempo y aumenta la formación del individuo.

La competencia Digital:

La competencia digital (CD) es aquella que implica el uso creativo, crítico y seguro de las tecnologías de la información y la comunicación para alcanzar los objetivos relacionados con el trabajo, la empleabilidad, el aprendizaje, el uso del tiempo libre, la inclusión y participación en la sociedad.

Esto conlleva el conocimiento de las principales aplicaciones informáticas y también el acceso a las fuentes, el procesamiento de la información y el conocimiento de los derechos y las libertades que asisten a las personas en el mundo digital. La persona ha de ser capaz de hacer un uso habitual de los recursos tecnológicos disponibles con el fin de resolver los problemas reales de un modo eficiente, así como evaluar y seleccionar nuevas fuentes de información e innovaciones tecnológicas, a medida que van apareciendo, en función de su utilidad para acometer tareas u objetivos específicos

Se trata de desarrollar una actitud activa, crítica y realista hacia las tecnologías y los medios tecnológicos, valorando sus fortalezas y debilidades y respetando principios éticos en su uso. Para el adecuado desarrollo de la competencia digital resulta necesario abordar:

- La información.

- La comunicación.
- La creación de contenidos.
- **La seguridad.**
- La resolución de problemas.

4.2 Las TIC en los objetivos generales de la LOMCE en la ESO y Bachillerato

Punto e) del Real Decreto 1105/2014, de 26 de diciembre, por el que se establece el currículo básico de la Educación Secundaria Obligatoria:

"e) Desarrollar destrezas básicas en la utilización de las fuentes de información para, con sentido crítico, adquirir nuevos conocimientos. Adquirir una preparación básica en el campo de las tecnologías, especialmente las de la información y la comunicación."

Punto g) del Real Decreto 1105/2014, de 26 de diciembre, por el que se establece el currículo básico de Bachillerato:

*g) Utilizar con **solvencia y responsabilidad** las tecnologías de la información y la comunicación*

4.3 La formación TIC del profesorado

Son numerosos los estudios que han analizado el impacto de las tecnologías de la información y la comunicación en el rol que desempeña el profesor en la adquisición de la competencia digital por parte de los alumnos. Bonel (2016) en su estudio destaca que la mayoría de docentes valora positivamente la integración de las nuevas tecnologías en la educación pero siempre que estas se vean reforzadas por un cambio metodológico y por una adecuada formación del profesorado.

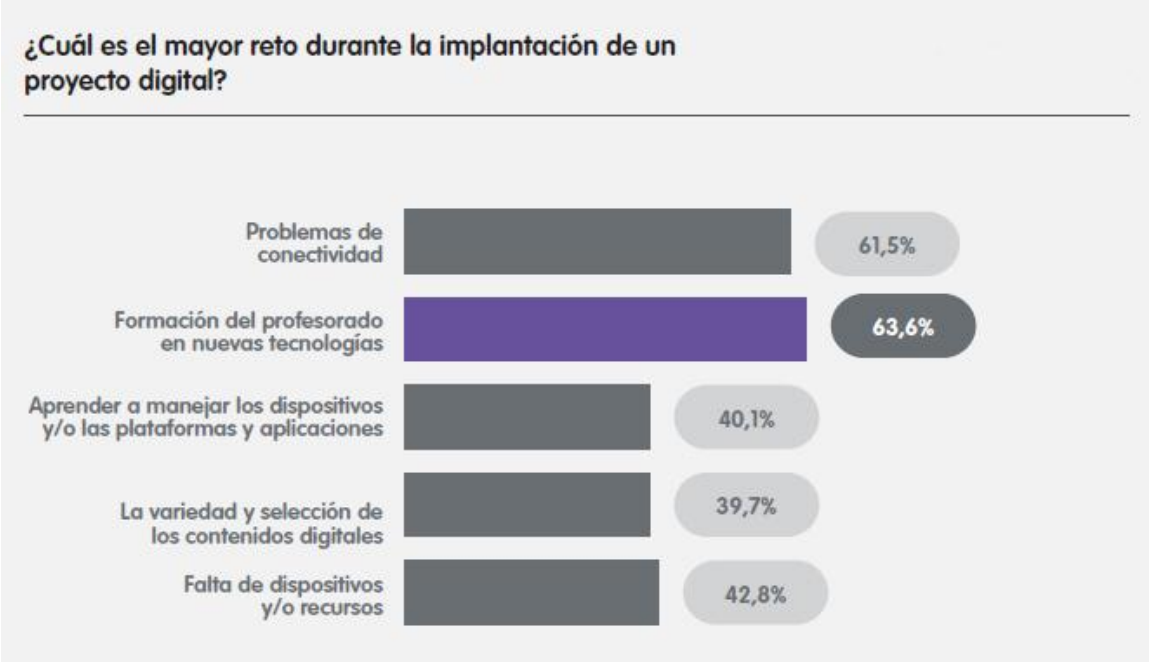
Para Fernández Sánchez (2017) una variable que sí parece repetirse en la mayoría de los casos analizados es que el éxito de la utilización de las TIC está muy relacionado con la presencia en los centros educativos de profesores emprendedores e innovadores. Si bien nos indica que no es el único, pues no debemos olvidarnos de factores como la formación, capacidad, la motivación, y los recursos del centro.

En cuanto a la formación específica en TIC de los docentes es en la evaluación de la información donde el docente de Secundaria presenta importantes deficiencias. Si bien

identifica bastante bien la información relevante de la que no lo es, tiene dificultades muy graves para discriminar en su correo electrónico entrante lo verdaderamente importante de lo que no lo es así como sustanciales dudas a la hora de dar fiabilidad y veracidad a la información que obtiene por la Red frente a la que puede obtener por recursos analógicos (Álvarez J.F., 2015).

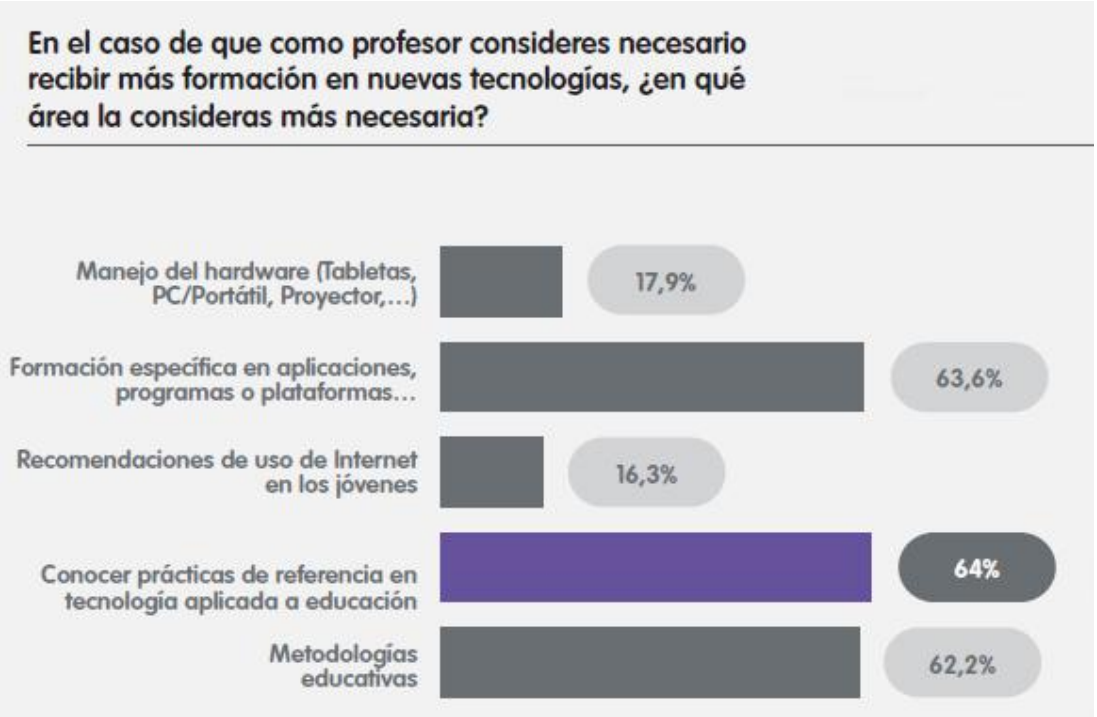
Para esclarecer un poco más la situación actual de los profesores con respecto a la integración de las TIC dentro del aula, hemos echado un vistazo al II Estudio Blink (Blink Learning, Universidad Juan Carlos Primero, 2016) sobre el uso de la tecnología en el aula, realizado con la ayuda de 740 docentes de España y Latinoamérica de centros públicos, privados y concertados, desde infantil hasta enseñanzas universitarias.

En dicho estudio se concluye que el 93 % de los docentes "recomienda iniciar un proyecto digital, pero siempre acompañado de un cambio metodológico" y que los principales desafíos que presenta el uso de la tecnología en el aula son: "la falta de formación del profesorado en el uso de las TIC (63,6 %) y la conectividad a internet de los centros educativos (61,5 %)". Por otro lado, aunque solo un 19 % de los profesores alude al uso de la tecnología como un déficit académico del alumnado, **un amplio porcentaje coincide en la necesidad de reforzar la formación en competencias digitales (70 %) y un uso responsable de internet (57 %).**



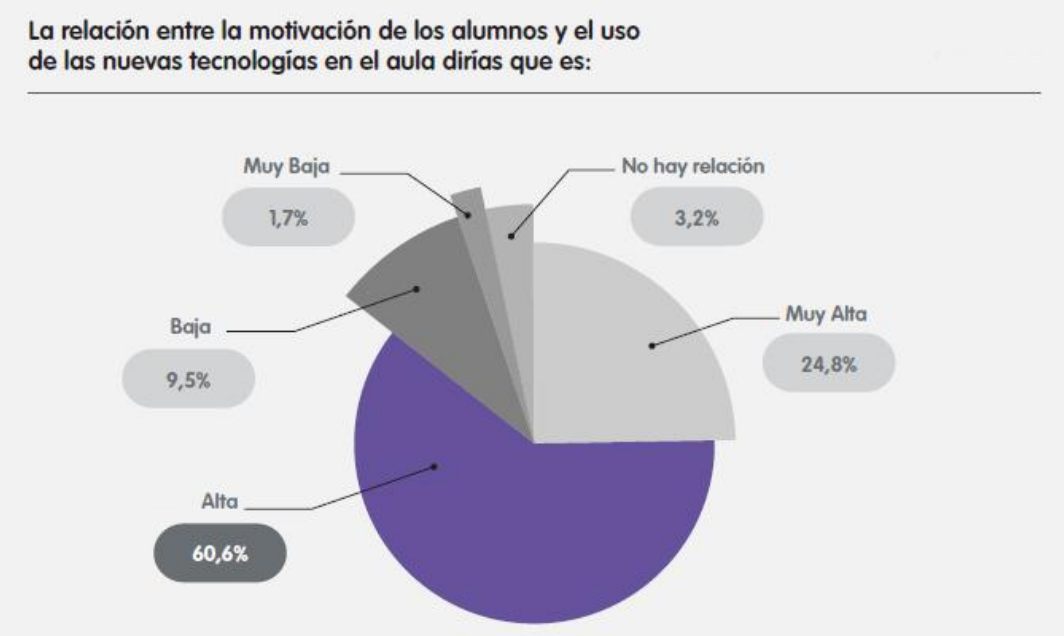
10. Estadísticas del informe Blink sobre los retos en la implantación de un proyecto digital

Y es que como señalan Blanco y Gimeno (2005), la tecnología por sí sola no basta para reforzar el proceso de enseñanza-aprendizaje. **La integración TIC teniendo como objetivo una mejora en el rendimiento de los alumnos pasa además por un cambio sustancial en metodologías, contenidos y procedimientos de evaluación**.

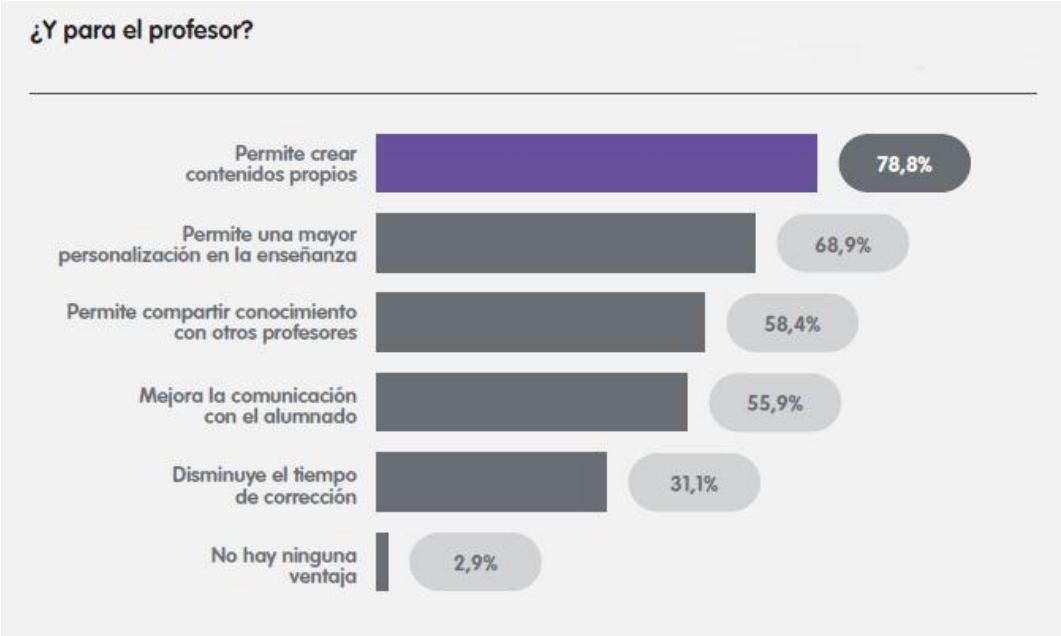


11. Estadísticas del informe Blink sobre la formación del profesorado en TIC

Como consecuencia de esta situación, y debido a la falta de formación del profesorado, existen en la actualidad **un gran número de docentes que no se sienten capacitados para un uso pedagógico de las TIC** puesto que desconocen como incorporarlo en los procesos de enseñanza-aprendizaje, formación que es aún más deficiente si se trata de producir y diseñar herramientas con un uso didáctico y cuándo el recurso tecnológico es novedoso (Fernández Sánchez, 2017).



12. **Estadísticas del informe Blink sobre la relación entre TIC y motivación en el aula.**



13. **Estadísticas del informe Blink sobre TIC y profesorado.**

Dicha formación debe ir en cualquier caso más allá de la mera instrucción en el uso y manejo de las herramientas, y abarcar aspectos como estilos de aprendizaje distintos, nuevas metodologías didácticas, auto-aprendizaje, etc., en definitiva, que **el uso de las TIC no sea simplemente un cambio en las formas y suponga en esencia un cambio en los procedimientos.**

4.4 Las TIC en el currículo de la ESO

Como hemos visto con anterioridad, las TIC a través de la competencia digital tienen un carácter transversal según el cual en teoría deben estar presentes (sin precisar cómo, cuanto, ni de qué manera) en todas las áreas de conocimiento. Sin embargo existen dos asignaturas que en distintos cursos de la ESO sí que afrontan las TIC como un contenido que se debe impartir, aprender y evaluar y son las asignaturas de Tecnología y de Tecnologías de la Información y la Comunicación.

Tecnología en 1º de la ESO:

Se trata de una asignatura específica **obligatoria para todos los alumnos**. Entre sus contenidos en el bloque 5 hay uno específico dedicado a las Tecnologías de la Información y la comunicación en el que se cursan los siguientes contenidos:

- Elementos que constituyen un ordenador.
- Unidad central y periféricos.
- Funcionamiento y manejo básico.
- El sistema operativo como interfaz persona-máquina. Almacenamiento, organización y recuperación de la información en soportes físicos, locales y extraíbles.
- Instalación de programas informáticos básicos.
- Internet: conceptos básicos, terminología, estructura y funcionamiento.
- El ordenador como medio de comunicación: Internet y páginas web.
- Herramientas para la difusión, intercambio y búsqueda de información.
- El ordenador como herramienta de expresión y comunicación de ideas: terminología y procedimientos básicos referidos a programas de edición de texto y de edición de presentaciones técnicas.
- **Seguridad básica en el uso de equipamiento electrónico e informático. Seguridad básica en la publicación e intercambio de información.**

Tecnología en 3º de la ESO:

Se trata de una asignatura específica pero esta vez **optativa**. Entre sus contenidos en el bloque 5 hay uno específico dedicado a las Tecnologías de la Información y la comunicación en el que se cursan los siguientes contenidos:

- El ordenador como medio de comunicación intergrupal: comunidades y aulas virtuales. Internet. Foros, blogs y wikis.
- El ordenador como herramienta de tratamiento de la información: Terminología y procedimientos básicos referidos a programas de hoja de cálculo y de base de datos.
- **Actitud crítica y responsable hacia la propiedad y la distribución del software y de la información: tipos de licencias de uso y distribución.**
- Introducción a la comunicación alámbrica e inalámbrica.
- Introducción a la telefonía, radio y televisión.
- **Medidas de seguridad y de protección personal en la interacción mediante entornos tecnológicos de intercambio de información y de comunicación.**

Tecnología en 4º de la ESO:

En la rama de Enseñanzas Aplicadas, se trata de una asignatura específica y **optativa**. Entre sus contenidos en el bloque 1 hay uno específico dedicado a las Tecnologías de la Información y la comunicación en el que se cursan los siguientes contenidos:

- Elementos y dispositivos de comunicación alámbrica e inalámbrica.
- Redes. Tipología.
- Publicación e intercambio de información en medios digitales.
- **Uso seguro y responsable de los medios de publicación e intercambio de información.**
- Conceptos básicos e introducción a los lenguajes de programación.
- Uso de ordenadores y otros sistemas de intercambio de información.
- Diseño asistido por ordenador: Herramientas CAD.

Tecnologías de la Información y la Comunicación. 4º de la ESO

Se trata de una materia específica **optativa** tanto para los alumnos de la rama de Enseñanzas Aplicadas como para la rama de Enseñanzas Académicas. Básicamente se dedica a ampliar y profundizar en los conocimientos que de ella el alumnado haya adquirido en cursos anteriores, enseñándole, a su vez, la forma de integrar estos aprendizajes con el resto de materias. Según la LOMCE ello le permitirá continuar sus estudios con éxito o incorporarse al mundo laboral con el grado adecuado de adquisición de la competencia digital. **Se trata de un contenido amplio y profundo que**

verdaderamente hace hincapié en temas de seguridad y de protección de datos que son de interés general para todos los usuarios. Como ejemplo en el bloque 1:

Bloque 1. Ética y estética en la interacción en red

- **Riesgos asociados a la interacción en la red: fraude, suplantación de identidad, pérdida de la privacidad, acceso a contenidos inadecuados y acoso.**
- Protección de la intimidad y la seguridad personal en la interacción en entornos virtuales.
- Estrategias para combatir el fraude, medidas de protección.
- **Encriptación y claves seguras. Certificados digitales y firma digital. DNI electrónico.**
- Descarga e intercambio de información: archivos compartidos en la nube, redes P2P y otras alternativas para el intercambio de documentos.
- La propiedad y la distribución del software y la información: software libre y software privativo, tipos de licencias de uso y distribución.
- Derechos de autor, copyright, licencias libres y *Creative Commons*. Situación actual.

4.5 Las TIC en el currículo de la Bachillerato

Tecnologías de la Información y la Comunicación 1º de la Bachillerato

Se trata de una materia específica **optativa** para los alumnos de todas las especialidades. Sus contenidos se organizan en los siguientes bloques:

- **Bloque 1. La sociedad de la información y el ordenador**
- Bloque 2. Arquitectura de ordenadores
- Bloque 3. Software para sistemas informáticos
- Bloque 4. Redes de ordenadores
- Bloque 5. Programación

Tecnologías de la Información y la Comunicación 2º de la Bachillerato

Se trata de una materia específica **optativa** para los alumnos de todas las especialidades. Sus contenidos se organizan en los siguientes bloques:

- Bloque 1. Programación

- Bloque 2. Publicación y difusión de contenidos
- **Bloque 3. Seguridad**

4.6 Reflexión sobre este apartado.

Una vez estudiado la Ley Orgánica para la Mejora de la Calidad Educativa y tras analizar como abordan los distintos currículos el tema de las TIC y su uso productivo, seguro y responsable, podemos decir que la LOMCE en los que respecta a las nuevas tecnologías de la información y la comunicación es en realidad un cascarón vacío.

Po un lado nos dice que van a ser fundamentales, pero a la hora de la verdad ni las desarrolla ni las toca, **sino que se quedan en el limbo de la transversalidad al no ser consideradas ni un medio imprescindible para la formación del alumnado y tampoco una disciplina a impartir** salvo en ocasiones excepcionales como en las materias de Tecnología y de Tecnologías de la Información y la Comunicación. En 1º de la ESO es el único curso en el que se garantiza que los estudiantes van a tener algo de formación específica en el uso y manejo de las TIC. En el resto de cursos que los estudiantes accedan o no a dicha formación va a depender de su elección pues se trata de materias optativas. Solo en Tecnologías de la Información y la Comunicación en 4º de ESO y en Bachillerato la formación que se da a los estudiantes se puede considerar completa y de calidad en lo que en materia de seguridad se refiere.

Sin embargo a lo largo de los currículos de las distintas materias la frase *"…..utilizando para ellos las tecnologías de la información y la comunicación"* es una constante en todo el documento. El texto las tiene siempre presentes pero jamás precisa o define qué se entiende por utilizarlas. Resulta demasiado ambiguo y completamente a merced de la interpretación del profesor que puede ser buena o no serlo en absoluto, sin menospreciar la labor docente.

En resumen, **se consideran las TIC como un complemento a la enseñanza y no como un medio para la misma**, obviando que en el entorno familiar de los estudiantes no todos pueden optar de la misma forma a los recursos tecnológicos y que además los docentes, padres y tutores, atropellados por la brusca irrupción en sus vidas del mundo digital, no tienen por qué tener la formación necesaria para enseñar de forma adecuada su uso tanto dentro como fuera del aula.

Nos encontramos en definitiva un alumnado muy diverso y desigual, **al que se le considera "nativo digital" y bajo esa etiqueta se le atribuyen destrezas en el uso de estas nuevas tecnologías que en realidad no posee, sobre todo en el campo de la responsabilidad y la seguridad**. Por todo ello, entre los alumnos que acceden a la formación profesional sobre todo en sus modalidades de Grado Medio o Básica existe una alta tasa de probabilidad de que muchos carezcan de conocimientos suficientes en la materia para incorporarse a una empresa en la que casi seguro de una manera u otra deberán utilizar un dispositivo tecnológico (en la mayoría de los casos un ordenador) con acceso a la red.

A colación de todo lo anterior, y puesto que el currículo no lo hace, parece lógico pensar que la formación en el uso seguro y responsable de las TIC debería de ser reforzada dentro de estos ciclos formativos para garantizar que los estudiantes accedan a las FCTs y a la empresa en las mejores condiciones posibles. Sin embargo antes de asegurarlo con rotundidad deberíamos comprobar cómo verdaderamente la Formación Profesional integra las TIC en sus currículos y eso es precisamente lo que vamos a analizar a continuación.

5. Las TIC en la Formación Profesional.

En la actualidad la mayoría de los títulos que se ofertan en la Formación Profesional son títulos LOE. Estos se encuentran amparados bajo LEY ORGÁNICA 2/2006, de 3 de mayo, de Educación en la que ya entonces se podía leer:

"La pretensión de convertirse en la próxima década en la economía basada en el conocimiento más competitiva y dinámica…"

"A la vista de la evolución acelerada de la ciencia y la tecnología y el impacto que dicha evolución tiene en el desarrollo social, es más necesario que nunca que la educación prepare adecuadamente para vivir en la nueva sociedad del conocimiento y poder afrontar los retos que de ello se derivan."

"…garantizar el acceso de todos a las tecnologías de la información"

Como podemos las TIC ya gozaban de una papel protagonista en los objetivos generales de la LOE. Esta reconoce que la sociedad está cambiando y por lo tanto la educación tiene que evolucionar con ella para que las nuevas generaciones sepan desenvolverse en el nuevo entorno socio-económico que se les presenta. Para poder ver como se traduce todo esto dentro de los currículos de los ciclos, hemos realizado un análisis de diversos títulos de distinto grado (FP Básica, Media y Superior) y de distintas familias profesionales. Veamos como enfocan la formación en las Tecnologías de la Información y la Comunicación cada uno de ellos.

5.1 Título profesional básico en Fabricación y Montaje

Viene regulado por la siguiente normativa:

- Real Decreto 127/2014, de 28 de febrero, Anexo III de donde se deriva la ORDEN EDU/515/2014, de 18 de junio, por la que se establece el currículo correspondiente al título profesional básico en Fabricación y Montaje en la Comunidad de Castilla y León.
- La Ley Orgánica 5/2002, de 19 de junio, de las Cualificaciones y de Formación Profesional

Identificación del título:

- **FAMILIA PROFESIONAL:** Fabricación Mecánica e Instalación y Mantenimiento.
- **DENOMINACIÓN:** Fabricación y Montaje.
- **NIVEL:** Formación Profesional Básica.
- **DURACIÓN:** 2.000 horas.
- **REFERENTE EUROPEO:** CINE-3.5.3 (Clasificación Internacional Normalizada de la Educación).
- **CÓDIGO**: FME01B.

Módulos profesionales del ciclo formativo:

- 3020. Operaciones básicas de fabricación.
- 3021. Soldadura y carpintería metálica.
- 3022. Carpintería de aluminio y PVC. 3023. Redes de evacuación.
- 3024. Fontanería y calefacción básica. 3025. Montaje de equipos de climatización.
- 3009. Ciencias aplicadas I.
- 3019. Ciencias aplicadas II:
- 3011. Comunidad y sociedad I.
- 3012. Comunidad y sociedad II.
- 3027. Formación en centros de trabajo

Aunque en apariencia ninguno de los módulos profesionales está directamente vinculado a las TIC, en todos ello se especifica entre los objetivos generales del módulo:

"Utilizar las tecnologías de la información y proponer formas de trabajo compartidas en las que los alumnos además de ayudarse unos a otros se acostumbren a defender sus opiniones con argumentos, escuchar a los demás, compartir las tareas y tolerar a sus compañeros."

El párrafo anterior es una prueba más de que las TIC siguen teniendo también en la Formación Profesional un carácter muy trasversal y ambiguo. En todos los módulos se especifica que se deben usar las TIC pero no indica cuanto, ni cómo, ni en qué profundidad. Además llama la atención como en la misma frase agrupa conceptos que en mi opinión no tienen que ver mucho unos con otros… "utilizar las tecnologías de la

información, formas de trabajo compartidas, ayudarse unos a otros, escuchar a los demás." Está hablando casi de valores, nunca de contenidos ni de formación concreta.

Sin embargo no ocurre lo mismo con los riesgos laborales y sus medidas de prevención asociadas, a los cuales se hace referencia en numerosos lugares aunque estos hacen alusión siempre a los trabajos en taller con las máquinas correspondientes. Y no podemos evitar preguntarnos **¿acaso la formación en el uso seguro y responsable de las Tecnologías de la Información y la Comunicación no sería en sí mismo una medida de prevención muy importante y necesaria para las empresas?**

Continuando con el estudio del currículo, en los módulos de Ciencias aplicadas I y II se especifica claramente:

"Se debe potenciar el uso de las tecnologías de la información y la comunicación. El ordenador puede utilizarse para buscar información, y para tratarla y presentarla."

Como podemos ver, las intenciones del currículo están claras, no obstante la palabra final acerca del cómo, cuanto y cuando la tiene de nuevo el docente. Sin embargo en el módulo de Comunicación y sociedad I y II sí que encontramos entre los contenidos alusión directa al uso y manejo de los TIC dentro del aula aunque no se trate de formación específica en temas de seguridad. Así por ejemplo tenemos:

- Tratamiento y elaboración de información para las actividades educativas:
  - Recursos básicos: resúmenes, fichas temáticas, biografías, hojas de cálculo o similares, elaboración, entre otros.
  - Búsqueda de información a través de internet.
  - Uso de repositorios de documentos, buscadores y enlaces web.
  - Vocabulario específico.
- Composiciones orales
  - Uso de medios de apoyo: audiovisuales y TIC
- Presentación de textos escritos en distintos soportes:
  - Instrumentos informáticos de software para su uso en procesadores de texto.

Debemos mencionar que los contenidos de estos módulos son muy variopintos y abarcan una gran cantidad de temas que van desde la historia o la lengua hasta, como vemos anteriormente, un manejo muy, muy básico de las TIC. Por su parte en las

orientaciones pedagógicas y metodológicas de este módulo se especifica que las líneas de actuación estarán orientadas hacia:

- La utilización de estrategias, recursos y fuentes de información a su alcance, fomentando el uso de las TIC, que contribuyan a la reflexión sobre la valoración de la información necesaria para construir explicaciones estructuradas de la realidad que le rodea.
- La selección y ejecución de estrategias didácticas que faciliten el auto-aprendizaje y que incorporen el uso de la lengua en situaciones de comunicación lo más reales posibles, utilizando las posibilidades de las Tecnología de la Información y de la Comunicación (correo electrónico, SMS, internet, redes sociales, entre otras).
- La garantía del acceso a la información para todos los alumnos, fomentando el uso de las TIC. Deberán tener una actitud crítica y reflexiva en la valoración de la información disponible, contrastándola cuando sea necesario, y respetando las normas de conducta acordadas socialmente para regular el uso de la información y sus fuentes en los distintos soportes.

En conclusión, poca inclusión de las TIC en los contenidos de este ciclo formativo y casi todo orientado hacia la búsqueda en internet y al uso de programas básicos de ofimática y nada respecto a la seguridad de cara el manejo de un dispositivo informático con acceso a la red dentro de la empresa.

5.2 Título de Técnico en Gestión Administrativa

Viene regulado por la siguiente normativa:

- Real Decreto 1631/2009, de 30 de octubre del que se deriva el DECRETO 66/2011, de 9 de diciembre, por el que se establece el currículo correspondiente al título de Técnico en Gestión Administrativa en la Comunidad de Castilla y León.
- La Ley Orgánica 5/2002, de 19 de junio, de las Cualificaciones y de la Formación Profesional.

Identificación del título:

- **FAMILIA PROFESIONAL:** Administración y Gestión.
- **DENOMINACIÓN:** Gestión Administrativa.
- **NIVEL:** Formación Profesional de Grado Medio.

- **DURACIÓN:** 2.000 horas.
- **REFERENTE EUROPEO:** CINE-3 (Clasificación Internacional Normalizada de la Educación).
- **CÓDIGO:** ADG01M

Módulos profesionales del ciclo formativo:

- 0437. Comunicación empresarial y atención al cliente.
- 0438. Operaciones administrativas de compra-venta.
- 0439. Empresa y Administración.
- 0440. Tratamiento informático de la información.
- 0441. Técnica contable.
- 0442. Operaciones administrativas de recursos humanos.
- 0443. Tratamiento de la documentación contable.
- 0156. Inglés.
- 0446. Empresa en el aula.
- 0448. Operaciones auxiliares de gestión de tesorería.
- 0449. Formación y orientación laboral.
- 0451. Formación en centros de trabajo.

Por la naturaleza de este ciclo formativo, en el que el ordenador es una herramienta de trabajo esencial para este perfil profesional, las TIC se encuentran muy integradas en todos los módulos profesionales siempre orientadas a las funciones que el trabajador debe desempeñar.

Así por ejemplo en el módulo Comunicación empresarial y atención al cliente nos encontramos con los siguientes contenidos:

- La informática en las comunicaciones verbales.
- Medios y equipos ofimáticos y telemáticos.
- **El correo electrónico.**
- **Aplicación de procedimientos de seguridad y confidencialidad de la información.**
- Archivo de la información en soporte informático
- La firma digital como sistema de seguridad en las comunicaciones mercantiles.

- Confidencialidad de la información y documentación.
- **Procedimientos de protección de datos.**
- Etc

Como podemos ver, dedican un capítulo específico al correo electrónico, donde podemos pensar que se abarca desde su configuración hasta el uso correcto del mismo y también a detectar elementos potencialmente peligrosos. Más interesante si cabe es el apartado dedicado a la aplicación de procedimientos de seguridad y confidencialidad de la información, y el de procedimientos de protección de datos que también puede dar mucho juego si el profesor quiere incidir en la importancia de la ciberseguridad con sus alumnos.

A pesar de que en los contenidos sí se refleja formación específica relacionada con la ciberseguridad, llama la atención que en los objetivos generales del módulo y en las orientaciones pedagógicas y metodológicas no viene este hecho precisado. Lo más parecido que nos encontramos, es que el módulo profesional contiene la formación necesaria para desempeñar las funciones relacionadas con la comunicación en la empresa, tales como:

- La recepción, tramitación y gestión de documentación.
- La elaboración, registro y archivo de documentación.

Por su parte, en el módulo de Tratamiento Informático de la Información, contiene toda la formación necesaria para desempeñar la función de instalación y explotación de aplicaciones informáticas de forma muy completa como por ejemplo.

- Instalación y actualización de aplicaciones
- Elaboración de documentos y plantillas mediante hojas de cálculo y procesadores de texto
- Utilización de bases de datos ofimáticas
- Integración de imágenes y vídeos en documentos, y presentaciones
- Gestión de correo y agenda electrónica

Esta vez sí, en el apartado de objetivos generales del ciclo con un objetivo que dice:

"Identificar las normas de calidad y seguridad y de prevención de riesgos laborales y ambientales, reconociendo los factores de riesgo y parámetros de calidad para aplicar los protocolos correspondientes en el desarrollo del trabajo."

Y también:

"Realizar documentos y comunicaciones en el formato característico y con las condiciones de calidad correspondiente, aplicando las técnicas de tratamiento de la información en su elaboración."

Aquí, esta vez sí donde leemos "riesgos laborales" podemos llegar a sobreentender que también se refiere a protocolos de seguridad en el tratamiento informático de la información.

En definitiva, por la naturaleza del perfil profesional a quien va destinado el ciclo formativo, era de esperar que esta vez sí, el uso seguro y responsable de las nuevas tecnologías tuviera presencia (y destacada) en los contenidos de varios de los módulos. No obstante se trata de un puesto de trabajo que irremediablemente hoy en día se debe realizar en su totalidad con un ordenador y una conexión a la red realizando funciones de gestión de la información y que esta es además sensible e importante para cualquier organización.

Por ello y para todos los ciclos formativos de esta familia profesional, sería el doble de interesante y necesario desarrollar una serie de actividades dirigidas a reforzar y también profundizar en todos estos conocimientos que resultarán esenciales para estos futuros trabajadores en sus tareas diarias.

5.3 Técnico Superior en Asesoría de Imagen Personal y Corporativa

Viene regulado por la siguiente normativa:

- Anexo I del Real Decreto 1685/2011, de 18 de noviembre del que se deriva el DECRETO 49/2015, de 23 de julio, por el que se establece el currículo correspondiente al título de Técnico Superior en Asesoría de Imagen Personal y Corporativa en la Comunidad de Castilla y León.
- La Ley Orgánica 5/2002, de 19 de junio, de las Cualificaciones y de la Formación Profesional.

Identificación del título:

- **FAMILIA PROFESIONAL:** Imagen Personal.
- **DENOMINACIÓN:** Asesoría de Imagen Personal y Corporativa.
- **NIVEL:** Formación Profesional de Grado Superior.
- **DURACIÓN:** 2.000 horas.
- **REFERENTE EUROPEO:** CINE-5b (Clasificación Internacional Normalizada de la Educación).
- **CÓDIGO:** IMP03S.
- **NIVEL DEL MARCO ESPAÑOL DE CUALIFICACIONES PARA LA EDUCACIÓN SUPERIOR:** Nivel 1 Técnico Superior.

Los módulos profesionales que componen el título:

- 1181. Asesoría cosmética.
- 1182. Diseño de imagen integral.
- 1183. Estilismo en vestuario y complementos.
- 1184. Asesoría de peluquería.
- 1185. Protocolo y organización de eventos.
- 1186. Usos sociales.
- 1187. Asesoría estética.
- 1188. Habilidades comunicativas.
- 1189. Imagen corporativa.
- 1071. Dirección y comercialización.
- 1190. Proyecto de asesoría de imagen personal y corporativa.
- 1191. Formación y orientación laboral.
- 1192. Empresa e iniciativa emprendedora.
- 1193. Formación en centros de trabajo.

Revisando los contenidos de los distintos módulos arriba mencionados, llama la atención la escasa referencia explícita a las TIC en este perfil profesional a pesar de que da la sensación de que absolutamente todo en los contenidos tiene que ver con ellas. Por ejemplo en el módulo profesional de Diseño de Imagen Integral se nos habla de:

- Métodos de obtención de la información: estrategias de búsqueda y selección.

- Actualización de la información: control, seguimiento y conservación.
- Diseño de documentos gráficos para la asesoría de imagen.

A estas alturas ya es sabido por todos que siempre que se hable de información está es casi siempre en formato "digital" que a bien seguro necesita ser almacenada y gestionada con aplicaciones y dispositivos informáticos. Por otro lado, parece razonable pensar que la información que pueda almacenar un asesor de imagen personal y también corporativa sea sensible y confidencial, suponiendo cualquier incidencia con la misma un riesgo severo para la credibilidad de dicho/a profesional u empresa.

Por lo tanto, los conocimientos en el tratamiento seguro y responsable de esa información, su almacenamiento ordenado y los protocolos seguros en su transmisión se convierten aquí en fundamentales y me resulta bastante curioso que esa formación se omita o se sobreentienda en los alumnos.

Lo más cerca que nos podemos encontrar relacionado con el uso seguro y responsable de Internet se encuentra en el módulo de Habilidades Comunicativas donde se nos habla de:

- Las nuevas técnicas de comunicación escrita: los e-mails, la netiqueta y otros.
- Fase de documentación. **Métodos de obtención de la información**: estrategias de búsqueda. Criterios de selección. Métodos de organización e integración de los resultados de la búsqueda. Análisis y clasificación de la información. Dossier de colaboradores profesionales: criterios para la elaboración y actualización de ficheros de especialistas.
- **Registro y control de la información. Cumplimentación y custodia de la documentación. Aplicación de la ley de protección de datos de carácter personal y normativa sobre el derecho a la imagen.**
- Tipos de soportes para la elaboración y preparación de documentos: papel, medios informáticos y medios audiovisuales, entre otros. Programas para realizar presentaciones.
- **Entrenamiento en herramientas de la comunicación:** teléfono, fax, comunicaciones escritas, internet, correo electrónico, utilización de blog y páginas Web entre otras. Tipos de lenguaje y técnicas que se deben emplear.

En el apartado de registro y control de la información sí que vemos se hace hincapié en la importancia de la custodia de la información. Como es lógico el alumno debe conocer de cerca los entresijos de las leyes de protección de datos, si bien esto no tiene mucho sentido si el futuro empresario o trabajador no conoce como almacenar y transmitir de forma segura toda esa información en formato digital.

En el último apartado se nos habla de "entrenamiento" en las herramientas de la comunicación teniendo especial importancia las de tipo digital como internet, correo electrónico, los blogs y las páginas web, etc. En mi opinión aquí existe una carencia importante y es la mención a las redes sociales. No puedo imaginarme un trabajador de este perfil profesional sin una adecuada formación en el uso productivo, eficaz y responsable de todas estas herramientas gratuitas que tenemos a nuestra disposición.

En definitiva veo las TIC como imprescindible para este puesto de trabajo y me parece que el currículo debería abordarlas de una forma más seria y profunda prestando especial anterior a los temas de seguridad.

5.4 Reflexión sobre este apartado

Analizando los currículos de los diferentes módulos lo primero que me llama la atención es la disminución de la alusión al término TIC según sube el grado del ciclo formativo. Es decir, a lo largo del currículo del TP Básico en Fabricación y montaje se pueden leer con frecuencia la frase *"se debe hacer uso de las tecnologías de la información"* mientras que en los títulos superiores, sobre todo en el Grado Superior, esto no ocurre en absoluto.

Obviamente, para poder afirmar esto con rotundidad, haría falta un estudio más extenso y meticuloso de todos los títulos ofertados por la formación profesional, sin embargo y dado lo visto hasta el momento, parece una hipótesis bastante plausible.

El por qué ocurre esto puede ser objeto de numerosas discusiones, si bien está claro que **cuanto mayor es la formación del alumno, más se le presupone que sabe utilizar las TIC como así viene especificado en la propia Competencia Digital**. Lo que no está tan claro es dónde, ni cómo ni quien le ha enseñado a hacerlo ni tampoco que ese manejo sea el más correcto. De hecho, como hemos podido comprobar, que un alumno finalice la ESO o incluso el Bachillerato no es garantía suficiente de que disponga unas nociones

sólidas y bien formadas en el uso de las TIC y mucho menos, que tenga conciencia de seguridad a nivel empresa.

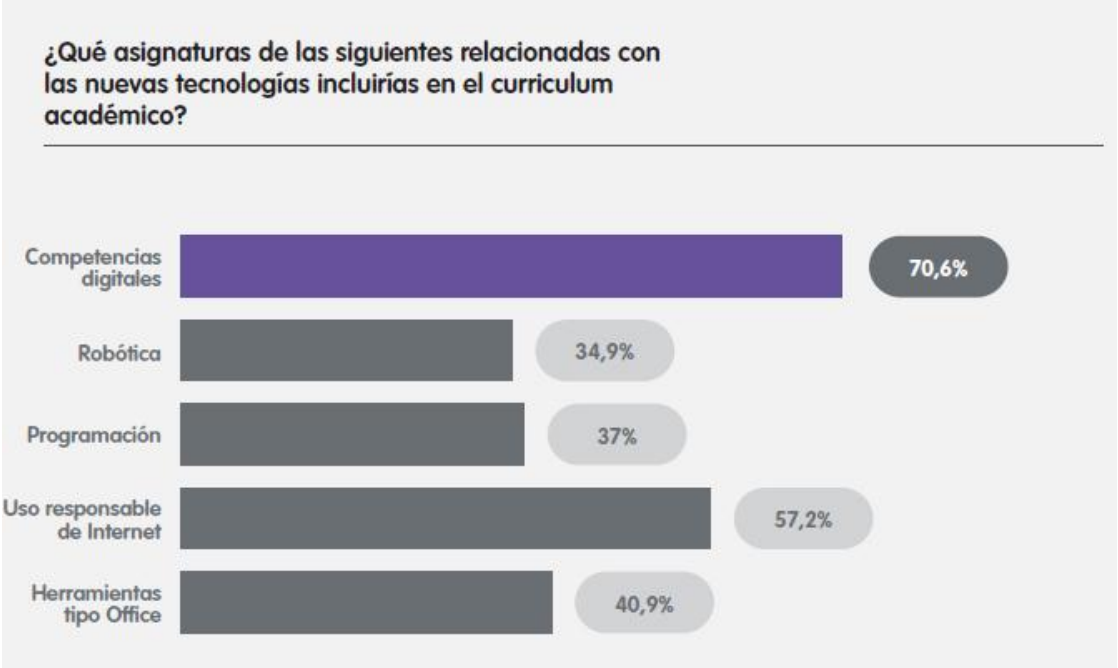
Y si los centros educativos no están formando adecuadamente a los alumnos en el uso y manejo de las TIC, ¿quién lo está haciendo? La respuesta es muy sencilla, y es que **padres y sistema educativo han caído en el error de atribuir a las nuevas generaciones la competencia digital por el mero hecho de ser "nativos digitales".**

Debemos tener en cuenta que utilizar las nuevas tecnologías no significa saber hacerlo de manera eficiente y responsable, de la misma forma que información no es conocimiento y que tener acceso a la información no significa necesariamente estar informado (Cabero, 2007).

Con respecto a los contenidos en materia de seguridad TIC impartidos dentro de los ciclos, podemos entrever que dependiendo del título y de la naturaleza del puesto de trabajo se hace más o menos hincapié en temas de seguridad. Pero en mi opinión, el sistema ha obviado que de una manera u otra, **hoy en día todos utilizamos las Tecnologías de la Información y la Comunicación de forma constante tanto para nuestra vida privada como profesional y que además los dispositivos que usamos para ello son en muchos casos los mismos.**

Los datos del último informe desarrollado por Telefónica lo avalan: cada vez más las empresas demandan a sus trabajadores más concienciación en temas de Ciberseguridad y sin embargo cada vez los usuarios son más descuidados. El sistema educativo no puede quedarse al margen de esta situación. Y así lo corroboran también los más de 700 profesores encuestados para el informe Blink que declararon necesaria la inclusión en el currículo de asignaturas específicas para el desarrollo de competencias digitales entre los alumnos (ver ilustración nº 14).

En definitiva, y como venía sucediendo en la ESO, la formación en competencia digital queda prácticamente reducida al ámbito de la transversalidad, con la incertidumbre y las dudas que ello plantea. **Si la formación profesional aspira verdaderamente a una enseñanza de calidad, la ciberseguridad y la formación en el uso seguro y responsable de las TIC deberían estar incluidas en el currículo**. De otro modo se estaría quedando al margen de los requisitos demandados por el mercado laboral como veremos a continuación.



14. Posibles nuevas asignaturas a incluir en el currículo académico relacionadas con las TIC.

6. Empresa y Ciberseguridad.

Según el informe *The State of Cybersecurity and Digital Trust* 2016 realizado por Accenture (ReasonWhy, 2017), el 69% de las empresas ha sufrido algún ciberataque durante el año 2016. Los principales objetivos: robo de datos, daños en los sistemas informáticos y extorsión.

Y es que como nos cuenta INCIBE (Instituto de la Ciberseguridad Español), a pesar de los avances tecnológicos de los últimos años y la aparición de sistemas de seguridad más eficaces, rápidos y modernos, está demostrado que **el elemento más importante para garantizar la seguridad dentro de una empresa de cualquier naturaleza, es siempre el empleado.**

Ello es debido a que los empleados son los encargados de gestionar, procesar, almacenar, modificar, transmitir y eliminar la información en una empresa y como tal deben conocer los riesgos potenciales asociados a dichas actividades y la desinformación y el desconocimiento son algunos de ellos. En caso contrario pueden llegar a adoptar actitudes de riesgo tan comunes como visitar una página maliciosa, desactivar el antivirus, ejecutar un archivo adjunto en el correo electrónico, utilizar un USB desconocido, etc.

A pesar de todas las medidas externas que se pueden adoptar por parte del departamento de informática (cortafuegos, sistemas de detección, acceso por huella, contenidos cifrados, contraseñas seguras, etc) el empleado al final necesita acceder a la información y trabajar con ella y está demostrado que la restricción severa es al final poco efectiva e incluso contraproducente pues acarrea problemas de productividad y ralentización.

La mejor solución por tanto, pasa por trabajar en la concienciación en materia de seguridad informática. Si se consigue, se evitarán así un gran número de amenazas y será entonces cuando serán verdaderamente efectivas las medidas necesarias para prevenir los riesgos externos restantes.

6.1 ¿Qué es lo que sería necesario reforzar?

Obviamente cada Ciclo Formativo, en función de la familia profesional a la que pertenezca y su perfil profesional, requiere de un refuerzo específico dirigido a las funciones que va a desempeñar el empleado en el puesto de trabajo. Sin embargo, siempre que el trabajador tenga acceso o requiera del uso de un ordenador para la realización de su

trabajo y que este disponga de acceso a internet, existen unos protocolos de actuación mínimos y comunes a cualquier profesión.

En el presente trabajo nos centraremos en realizar una serie de actividades que vayan enfocadas a este tipo de concienciación general y que serán aplicables a todos los ciclos formativos en cualquiera de sus niveles, básica, media y superior.

La plataforma INCIBE proporciona a las PYMES servicios en el ámbito de la ciberseguridad que permitan el aprovechamiento seguro de las TIC. En concreto se dedican a trabajar desde la prevención promoviendo el avance de la cultura de la seguridad de la información a través de la concienciación, la sensibilización y la formación.

Según este organismo el programa básico de concienciación para los usuarios pasa por la formación en 4 pilares básicos:

- Seguridad en el tratamiento y procesado de la información.
- Seguridad en el uso de los soportes de almacenamiento.
- Seguridad básica en nuestro terminal diario de trabajo.
- Seguridad en el uso de los dispositivos móviles.

6.2 ¿Dónde incluiríamos esa formación?

Sin duda esta ha sido el apartado del trabajo en torno al cual se ha generado más discusión y polémica. Para decidir cuál era la manera de introducir los contenidos citados arriba, se ha contado con la opinión de varios profesores de la formación de profesional, concretamente en el centro en donde tuve oportunidad de realizar las prácticas del máster y también con algún profesor ya retirado además de, por supuesto, la opinión del tutor del presente trabajo.

La pretensión inicial es que, siempre que sea posible, se debe incluir este tipo de actividades dentro del módulo que resulte más afín del ciclo formativo y en el caso de no existir ninguno que lo sea en apariencia, entonces se debería buscar dentro del currículo de alguno de los módulos un resquicio donde pudiera tener acogida. Ello no debería de ser demasiado costoso pues hoy en día existen numerosos apartados en los que de manera más o menos explícita se realizan alusiones a las TIC y/o a los elementos de seguridad.

Sin embargo los profesores del CIFP Simón de Colonia plantearon la posibilidad de realizar esta formación a través de una actividad complementaria pues les parecía que en muchos casos la inclusión vía currículo iba a resultar demasiado forzada y que además iba a obligar al profesor de dicho módulo a impartir una formación que casi seguro excedía sus capacidades docentes. Debo decir que yo personalmente en principio era partidaria de esta última opción, si bien finalmente y escuchando los consejos del tutor del presente trabajo finalmente tomé partido por la primera, es decir, de entre los módulos que pudieran ser más compatibles con dicha formación, se deberá buscar al profesor que por su perfil o disposición pudiera ser el más adecuado para impartir estos contenidos dentro de alguna UT que tuviera relación con el uso y manejo de las TIC.

Así por ejemplo en el caso del título profesional básico en Fabricación Mecánica e Instalación y Mantenimiento, veo factible su encaje dentro del módulo Comunicación y Sociedad II que se da en segundo curso antes de acceder a las CFTs y en que entre otras cosas se trata la búsqueda de información en internet, el uso de procesadores de texto, la creación de archivos audiovisuales, etc.

En el caso del título de Técnico en Gestión Administrativa, que es un ciclo formativo de grado medio para el que resulta especialmente interesante toda esta formación debido a su perfil profesional, tenemos el módulo de Tratamiento informático de la información en donde tendría muy buena acogida.

Finalmente, en el caso del título de Técnico Superior en Asesoría de Imagen Personal y Corporativa no existe ningún módulo que en principio sea muy obvia su inclusión pero leyendo el currículo del título su lugar podría ser el módulo de Diseño de Imagen Integral, en donde se nos habla de métodos para la obtención de la información, estrategias de búsqueda y selección o el de Habilidades Comunicativas también podría ser un lugar aceptable pues abarca el tema de redes sociales, etc.

7. Propuesta de actividades.

Como ya hemos dicho con anterioridad la idea es diseñar una serie de actividades de carácter general en materia de ciberseguridad básica para completar la formación de los alumnos en el uso seguro y responsable de las TIC en su puesto de trabajo sin importar cuál sea la naturaleza de este. Del mismo modo también **trataremos que las actividades sean fácilmente adaptables al contexto de los alumnos según la familia profesional a la que pertenezcan y también al tipo de ciclo formativo** (básico, medio o superior) que estén cursando.

Según el Kit de Concienciación de INCIBE, que forjará la base de nuestras actividades, la formación esencial para los usuarios consiste en 4 pilares básicos que serán nuestro punto de partida para comenzar a trabajar con los alumnos:

- Seguridad en el tratamiento y procesado de la información.
- Seguridad en el uso de los soportes de almacenamiento.
- Seguridad básica en nuestro terminal diario de trabajo.
- Seguridad en el uso de los dispositivos móviles.

La idea es que cada apartado se estructure de una forma similar y que tenga un máximo de 2 horas de duración. Cada sesión comenzará con la visualización conjunta de toda el aula de un video que tiene que ver con el tema a tratar, después de la cual se hará una pequeña puesta en común entre los alumnos para ver lo que piensan y abrir un debate de unos 15-20 minutos.

A continuación se pedirá a los alumnos que uno por uno piensen y luego digan en voz alta un consejo o medida preventiva que ellos piensan sería importante a tener en cuenta dentro de la empresa según el video y la discusión entre sus compañeros.

Finalmente se realizará el resto de actividades y a medida que estas se vayan completando se irán añadiendo "consejos" a nuestra lista o mejorando los existentes para que al final de la sesión los alumnos tengan una especie de decálogo de "buenas prácticas y conductas" en el tema a tratar. Al finalizar la sesión se entregará a los alumnos como recuerdo una serie de apuntes, trípticos, etc que tiene preparados y ofrece gratuitamente INCIBE y que completan la formación impartida en el aula.

La metodología de las sesiones estará centrada en el desarrollo de una dinámica interactiva como base para la reflexión y el debate grupal sobre el alcance y los efectos que la Red puede tener sobre la integridad de una empresa. Se plantearán **actividades inspiradas en el trabajo cooperativo** con el alumnado como protagonista, para que sean ellos mismos quienes vayan descubriendo las principales medidas de prevención en cada campo. Por otro lado, también se realizará alguna actividad de carácter práctico que siempre resultan amenas y nos permitirán poner en práctica lo aprendido en clase.

Para más información de cada una de estas actividades se puede consultar el Anexo I del presente trabajo.

7.1 Evaluación de los resultados

Evaluaremos nuestras actividades de tres maneras distintas. En primer lugar al finalizar todas las sesiones se realizará a los alumnos un sencillo test sobre cuestiones fundamentales en materia de ciberseguridad con el objetivo de evaluar la adquisición de los nuevos conocimientos. A continuación se les pedirá cumplimentar un cuestionario para conocer su opinión y la del profesor sobre este tipo de formación: si les ha resultado interesante, si lo encuentran útil para su futura profesión o para su vida personal, etc.

El siguiente test se trata tan solo de un ejemplo, en la práctica se deberán adaptar las preguntas al nivel de los alumnos y los contenidos que en concreto se hayan impartido:

EJEMPLO DE TEST DE EVALUACIÓN

1. **¿Qué es la información confidencial?**

   a) Aquella información que requiere aplicar medidas de seguridad para evitar su difusión. No importa el soporte, el tipo de información o si se ha comunicado verbalmente.

   b) Una norma de seguridad reconocida internacionalmente.

   c) Aquella información que no requiere aplicar medidas de seguridad para evitar su difusión. No importa el soporte, el tipo de información o si se ha comunicado verbalmente.

   d) Aquella información que requiere aplicar medidas de seguridad para evitar su difusión. No importa el soporte, el tipo de información pero no aplica a la información comunicada verbalmente.

2. **Un dato personal es**

a) Una fotografía.

b) Un DNI.

c) Un historial médico.

d) Todas las anteriores.

3. El cifrado de información…

a) Permite codificar cualquier contenido digital y hacerlo ilegible a terceras personas que no dispongan de la clave de descifrado.

b) Es una técnica que utiliza una base matemática.

c) Permite proteger la información en formato electrónico.

d) Todas las anteriores.

4. ¿Qué tipos de copias de seguridad existen?

a) Copias completas y graduales.

b) Copias completas, diferenciales y graduales.

c) Copias diferenciales, incrementales y completas.

d) Copias incrementales y diferenciales.

7. Respecto a las contraseñas de acceso…

a) Es útil utilizar la misma para varias aplicaciones o sitios de internet.

b) Los gestores de contraseñas son útiles para crear contraseñas seguras y recordar las diferentes contraseñas que podamos tener para cada aplicación o sitio de internet.

c) Utilizar una contraseña con información personal como fechas, nombres o palabras conocidas es seguro y además fácil de recordar.

d) Ninguna de las anteriores.

8. ¿Qué es un soporte de información?

a) Un dispositivo que nos permite almacenar información en formato papel.

b) Un dispositivo que nos permite almacenar fotografías y vídeos.

c) Un dispositivo que nos permite almacenar información en formato electrónico.

d) Ninguna de las anteriores.

9. ¿Qué medidas de seguridad se deben tomar para proteger un soporte y su información?

a) Hacer una copia de seguridad de su información.

b) Establecer una contraseña de acceso.

c) Cifrar su contenido.

d) Todas las anteriores son buenas medidas.

10. Si nos encontramos con un USB ¿Qué debemos hacer?

a) Abrirlo para ver si por el contenido podemos identificar a su propietario y devolvérselo

b) Abrirlo y cotillear los archivos que hay dentro

c) Llevarlo al departamento de informática para que sean los encargados de abrirlo de una forma segura

d) Jamás debemos utilizarlo.

11. ¿Cuál de las siguientes es una contraseña segura?

a) australia2018

b) Holamundo

c) 94o2nxti

d) lpazos$78

e) Ninguna de las anteriores

12. ¿Qué es un método de autenticación?

a) Un sistema para evitar que otros te reconozcan

b) Un mecanismo para publicar información en internet

c) Método por el cual obtener información confidencial

d) Técnica para verificar que un usuario es quien dice ser

e) Todas las anteriores

13. Cuando usamos redes WiFi públicas es recomendable

a) Manejar información sensible o confidencial

b) Utilizarlas para acceder a nuestra cuenta bancaria

c) Acceder a recursos corporativos

d) Ninguna de las anteriores

14. ¿Qué es BYOD?

a) Una tendencia que se basa en que los empleados hagan uso de sus dispositivos personales en el trabajo

b) Buy Your Own Device (Compra tu propio dispositivo)

c) Una tendencia que se basa en que los empleados no hagan uso de ningún dispositivo personal en el trabajo

d) Break Your Own Device (Rompe tu propio dispositivo)

15. Cuando recibimos un correo electrónico

a) No debemos abrir los archivos comprimidos si no conocemos al remitente.

b) No debemos hacer link en los enlaces que incluya si no conocemos al remitente.

c) Debemos desconfiar si el email tiene faltas de ortografía.

d) Todas las anteriores son verdaderas.

A continuación se expone un ejemplo de un posible cuestionario para conocer la opinión que tienen los alumnos sobre este tipo de actividades. Para ello se ha elaborado una tabla en la que el alumno deberá puntuar cada aspecto a valorar desde 1 a 5, siendo 1 cuando no se está de acuerdo con la afirmación planteada y 5 cuando se está totalmente de acuerdo:

	1	2	3	4	5
Las actividades me han parecido interesantes y útiles para mi futura profesión					
Las actividades me han parecido interesantes y útiles para mi vida privada					
Las sesiones han sido entretenidas y amenas					
Recomendaría este tipo de actividades a alumnos de otros Ciclos de Formación Profesional					
Ya disponía de conocimientos en Seguridad de la Información pero las actividades me han ayudado a reforzar lo que ya sabía					
Las actividades han conseguido cambiar alguno de mis hábitos respecto a la ciberseguridad (creación de constraseñas más seguras, uso de gestores de contraseñas, creación de copias de seguridad más amenudo, etc)					
En general soy consciente de los principales peligros que supone la red para mi información personal y para la de mi empresa					
Considero que con lo aprendido soy capaz de evitar situaciones y comportamientos de riesgo					

¿Tienes alguna sugerencia que hacernos? Por favor, escríbela

Por último se expone un ejemplo de un posible cuestionario para conocer la opinión del profesor sobre la experiencia realizada. Para ello de nuevo se ha elaborado una tabla en que deberá puntuar cada aspecto a valorar desde 1 a 5, siendo 1 cuando no se está de acuerdo con la afirmación planteada y 5 cuando se está totalmente de acuerdo:

	1	2	3	4	5
Los alumnos han mostrado interés y han participado activamente en las sesiones					
Los alumnos ya tenían conocimientos en materia de Seguridad de la Información					
Los vídeos han resultado entretenidos y claros					
El material facilitado por INCIBE ha resultado útil para la preparación de las sesiones					
El profesor considera que los alumnos han aumentado los conocimientos y la concienciación en Seguridad de la Información					
Recomendaría este tipo de actividades para alumnos de otros Ciclos Formativos					
Ha sido sencillo adaptar las actividades al contexto del alumnado según el título que están estudiando					

¿Tienes alguna sugerencia que hacernos? Por favor, escríbela

8. Conclusiones finales.

Una vez llegados a este punto lo verdaderamente interesante hubiera sido poder llevar a la práctica las sesiones arriba descritas. Sin embargo ello no ha sido posible pues en el momento de desarrollarse el presente trabajo ya no me encontraba en periodo de prácticas. Este trabajo, por lo tanto, queda abierto a una posible continuación el año que viene lo cual resultaría interesante sobre todo viendo que se trata de un tema de máxima actualidad en los tiempos que corren. Decir también que las actividades que aquí se han planteado son sólo meramente orientativas. En la práctica deben desarrollarse en función de numerosos factores como son, el contexto en el que se encuentra el centro, el nivel del ciclo formativo o la familia profesional a la que pertenece.

Por otro lado, creo poder decir que sí que ha quedado demostrado el por qué es necesario reforzar los conocimientos y la formación en ciberseguridad en los alumnos en general y en los de formación profesional en particular. Por un lado porque son las propias empresas quienes lo están demandando y por otro porque el sistema educativo no se está haciendo cargo de la tarea de forma comprometida, recayendo finalmente esta responsabilidad en los profesores y familiares quienes, como ya hemos visto, no tienen por qué tener la formación adecuada para hacerlo.

El presente trabajo concluye pues con la detección de 3 carencias básicas que tiene la actual ley de educación y que en mi opinión están ralentizando la integración plena de las TIC en las aulas y al mismo tiempo mermando su capacidad para mejorar la educación desde el fondo y no sólo desde la forma, como critican expertos y educadores.

En primer lugar detectamos la necesidad básica de **incluir en el currículo de los alumnos de la ESO una materia de carácter obligatorio o troncal que se dedique en exclusiva al desarrollo de las competencias digitales** para garantizar que todos los alumnos acceden a las oportunidades que brinda el mundo digital de una forma igualitaria y sin discriminaciones.

En segundo **lugar la formación en TIC del profesorado**, que sigue siendo la gran cuenta pendiente del sistema educativo, ya que como dice Fernández Sánchez (2017) su papel resulta fundamental para que la utilización de las TIC en las aulas se convierta en una verdadera oportunidad de mejora de los procesos de enseñanza-aprendizaje, puesto que la forma en que

el profesorado las utiliza es lo que hace de estos recursos una herramienta útil y productiva en la enseñanza.

En tercer y último lugar, **la inclusión de formación específica sobre ciberseguridad dentro de la formación profesional** para que todos los alumnos puedan reforzar sus conocimientos en la materia, haciéndoles más competitivos y atractivos para las empresas a la vez que les dotamos de mejor preparación para el desempeño de sus futuros trabajos.

En resumen, hay que tener presente que los requisitos del mercado laboral en este y otros temas son cada día más exigentes y obligan a la sociedad a adaptarse con rapidez a las nuevas circunstancias emergentes bajo la amenaza continua de la exclusión. El sistema educativo tiene por tanto la obligación de facilitar al alumno una base sólida sobre la que este pueda ir construyendo y ampliando su propio conocimiento. Y en esa búsqueda constante de la renovación y la mejora continua, la formación en competencias digitales, entre las que se encuentra el uso seguro y responsable de Internet, es sin lugar a dudas uno de los pilares fundamentales necesarios para poder desenvolverse con éxito en la nueva sociedad de la información.

9. Referencias.

- Elboj, C., Espanya, M., Flecha, R., Imbernon, F., Puigdellívol, I., y Valls, R. (1998). Comunidades de aprendizaje: Sociedad de la información para todos (cambios sociales y alguna propuesta educativa). *Contextos educativos*, 53-75.
- Aguilar Ramos, M. C., y Leiva Olivencia, J. J. (2012). La participación de las familias en las escuelas TIC: análisis y reflexiones. *Revista de Medios y Educación*, 7-19.
- Fernández, E.G.(2017). Papel del docente de Secundaria en la utilización de las TIC en el aula. En Ruiz-Palmero, J., Sánchez-Rodríguez, J. y Sánchez-Rivas, E. (Edit.). *Innovación docente y uso de las TIC en educación*. Málaga: UMA Editorial.
- Ferrer Soria, G. (2014). Las TIC en la LOMCE o una LOMCE con TiCs. *Fórum Aragón*, nº 19.
- Älvarez J.F., Gisbert M. (2015). Grado de alfabetización informacional del profesorado de Secundaria en España: Creencias y autopercepciones. *Comunicar*, nº 45.
- Cabero, J. (2007). Las nuevas tecnologías en la Sociedad de la Información. Recuperado de: https://www.researchgate.net/publication/238672345_Las_nuevas_tecnologias_en_la_Sociedad_de_la_Informacion
- Blink Learning, Universidad Rey Juan Carlos. (2016). II Estudio sobre el uso de la tecnología en el aula. Recuperado de: https://blinklearning1.blob.core.windows.net/tmp/BLINK_informe_TIC_2016.pdf
- Fundación Telefónica. (2017). La sociedad de la información en España 2016. Recuperado de: https://www.fundaciontelefonica.com/arte_cultura/sociedad-de-la-informacion/informe-sie-espana-2016/
- Fundación Telefónica. (2018). La sociedad digital en España 2017. Recuperado de: https://www.fundaciontelefonica.com/arte_cultura/sociedad-de-la-informacion/sdie-2017/
- Poncini H. (2018). El País: 'Cibercooperantes': los voluntarios contra el mal uso de Internet. Recuperado de: https://politica.elpais.com/politica/2018/05/14/actualidad/1526308853_502565.html
- Bonel,L. (2016). Heraldo:¿Qué opinan los profesores sobre el uso de las TIC en el aula?. Recuperado de http://www.heraldo.es

- (2017). ReasonWhy: Qué consecuencias puede tener un ciberataque para tu empresa. Recuperado de: https://www.reasonwhy.es.
- Ministerio de educación cultura y deporte. (2018). Competencias clave. Recuperado de: https://www.mecd.gob.es/educacion/mc/lomce/el-curriculo/curriculo-primaria-eso-bachillerato/competencias-clave/competencias-clave.html
- Ministerio de educación cultura y deporte. (2018). Títulos LOE. Recuperado de: http://www.todofp.es/que-como-y-donde-estudiar/que-estudiar/familia/loe.html
- Instituto nacional de ciberseguridad de España. (2018). Kit de concienciación. Recuperado de: https://incibe.es
- Real Decreto 1147/2011, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo.
- Ley Orgánica 2/2006, de 3 de mayo de Educación.
- Ley Orgánica 8/2013, LOMCE.
- RD 1105/2014 de 16 de diciembre por la que se establecen los objetivos de la ESO y del Bachillerato.
- ORDEN ECD/65/2015 de 21 de enero por la que se describen las relaciones entre las competencias, los contenidos y los criterios de evaluación.
- ORDEN EDU/363/2015, de 4 de mayo, por la que se establece el currículo y se regula la implantación, evaluación y desarrollo del bachillerato en la Comunidad de Castilla y León.
- Real Decreto 127/2014, de 28 de febrero, Anexo III de donde se deriva la ORDEN EDU/515/2014, de 18 de junio, por la que se establece el currículo correspondiente al título profesional básico en Fabricación y Montaje en la Comunidad de Castilla y León.
- Real Decreto 1631/2009, de 30 de octubre del que se deriva el DECRETO 66/2011, de 9 de diciembre, por el que se establece el currículo correspondiente al título de Técnico en Gestión Administrativa en la Comunidad de Castilla y León.
- Anexo I del Real Decreto 1685/2011, de 18 de noviembre del que se deriva el DECRETO 49/2015, de 23 de julio, por el que se establece el currículo correspondiente al título de Técnico Superior en Asesoría de Imagen Personal y Corporativa en la Comunidad de Castilla y León.

UNIVERSIDAD DE BURGOS

MÁSTER UNIVERSITARIO EN PROFESOR DE EDUCACIÓN SECUNDARIA OBLIGATORIA Y BACHILLERATO, FORMACIÓN PROFESIONAL Y ENSEÑANZA DE IDIOMAS

TRABAJO FIN DE MÁSTER. CURSO 2017- 2018

ANEXO I: Propuesta de actividades

Cristina de la Peña Acero

Especialidad: Tecnología Industrial

Tutor: David Hermindo Martín Alonso

Facultad de Educación

Contenido

1. Diseñando las actividades

1. Póster motivación INCIBE.

1.1 Actividad 1: Seguridad en el tratamiento y procesado de la información.

Objetivos

- Ser conscientes del interés que tiene nuestra vida privada para los demás.
- Reconocer quién puede llegar a acceder a la información que se comparte.
- Establecer medidas para proteger la información compartida en Internet.
- Reconocer correos electrónicos potencialmente peligrosos
- Reconocer cuándo y cómo cifrar la información
- Conocer la importancia de realizar copias de seguridad.

Resumen

Hacerse conscientes de la importancia de cuidar la importancia de la información que se transmite a través de Internet y de cómo hacerlo en las condiciones más seguras posibles minimizando los riesgos potenciales.

Metodología

Centrada en el desarrollo de una dinámica interactiva como base para la reflexión y el debate grupal sobre el alcance y los efectos que la Red puede tener sobre la información sensible tanto personal como de una empresa. Se plantea un trabajo cooperativo con el alumnado como protagonista, para que sean ellos quienes vayan descubriendo las pautas para compartir información de manera segura.

Materiales

- Equipo audiovisual con Internet para el grupo.
- Equipos informáticos conectados a Internet para cada participante.
- Apuntes impresos para los alumnos a modo de recuerdo propiedad de INCIBE

Estructura de la sesión

Comenzaremos la clase con la visualización de un vídeo de concienciación con la importancia de la información y cómo nos puede afectar de forma personal.

https://www.youtube.com/watch?v=NPE7i8wuupk

Preguntas para guiar el debate posterior:

- Tus dispositivos almacenan mucha información privada ¿Te habías parado a pensarlo?
- ¿Verdaderamente creéis que nos están espiando? ¿Para qué?
- Desde el punto de vista de una empresa ¿Qué es la confidencialidad?
- ¿Qué se puede hacer para asegurarse que la información que maneja una empresa es confidencial?

Comienzo de la ronda de posibles consejos y sugerencias en materia de tratamiento seguro de la información. Mientras el profesor va tomando nota de los mismos en la pizarra.

A continuación se dividirá la clase en grupos y a cada uno se le encargará la visualización de un vídeo. Tras su visualización los miembros del grupo discutirán sobre lo que han visto y lo traducirán en medias de seguridad que añadir o modificar a las existentes en la pizarra. Cuando todos los grupos hayan terminado cada grupo expondrá a los demás cuáles son sus medidas añadidas a la lista y por qué.

Video/Grupo 1: sobre el uso seguro y responsable del correo electrónico.

https://www.youtube.com/watch?v=7HjDyI4SCvA

Video/Grupo 2: Backup, la primera línea de defensa

https://www.youtube.com/watch?v=kW6RpKSo7xQ&list=PLr5GsywSn9d_hd7MTimziiM8yZH1d-Igz&index=23

https://www.youtube.com/watch?v=w2aZmRwhgio&list=PLr5GsywSn9d_hd7MTimziiM8yZH1d-Igz&index=1

Video/Grupo 3: Cifrado

https://www.youtube.com/watch?v=L3pVeyEPCy4

https://www.youtube.com/watch?v=wcJBmoz6Vlk

Para finalizar la sesión se realizará la puesta en común final y las conclusiones. Se realizarán los últimos retoques a las medidas de seguridad expuestas por los alumnos y se repartirá la documentación de INCIBE.

2. Algunas de las medidas imprescindibles sobre la seguridad en el tratamiento y procesado de la información.

1.2 Actividad 2: Seguridad en el uso de soportes de almacenamiento.

Objetivos

- Conocer los distintos tipos de soportes de información y sus riesgos.
- Saber cómo se destruye de forma segura un soporte.
- Saber cómo borrar de forma segura la información de un soporte.
- Conocer la diferencia entre cifrar y poner una contraseña a un dispositivo y saber realizarlo.

Resumen:

Conocer los dispositivos más habituales de almacenamiento de los que suele poseer una empresa y cómo gestionarlos de forma segura.

Metodología:

Se plantea un trabajo cooperativo con el alumnado como protagonista, para que sean ellos quienes vayan descubriendo las pautas en el uso responsable de dispositivos de almacenamiento portables. También se realizará una pequeña práctica en la que el alumno aprenderá a proteger mediante contraseña un USB propio, y también a cifrar su contenido y borrar la información de forma segura.

Materiales:

- Equipo audiovisual con Internet para el grupo.
- Equipos informáticos conectados a Internet para cada participante.
- USB propios de cada alumno.
- Apuntes impresos para los alumnos a modo de recuerdo propiedad de INCIBE

Estructura de la sesión:

Comenzaremos la clase con la visualización de un vídeo que nos ilustra sobre los distintos tipos de soportes informáticos en la actualidad:

https://www.youtube.com/watch?v=Qsunfh8DXD0

Preguntas para guiar el debate posterior:

- ¿Qué tipos de soportes usan los alumnos en su vida personal y para qué?
- ¿Están dotados de alguna medida de seguridad?
- ¿Qué riesgos asociados a estos dispositivos debemos tener en cuenta?

Teniendo en cuenta lo aprendido en la sesión anterior y la presente, se comienza la ronda de posibles consejos y sugerencias en materia de uso seguro y responsable de los distintos tipos de soportes. El profesor irá tomando nota en la pizarra de los mismos.

A continuación se realizará la práctica con las memorias USB bajo la supervisión del profesor. Este procederá a establecer una contraseña para el dispositivo, a continuación cifrará la información contenida mediante un programa de cifrado gratuito descargado de internet y por último mostrará como borrar la información de forma segura. Los alumnos podrán seguir las explicaciones viendo la pantalla del profesor con ayuda del programa ITALC y a la vez lo irán realizando ellos mismos en sus USBs.

Para finalizar la sesión se realizará la puesta en común final y las conclusiones. Se realizarán los últimos retoques a las medidas de seguridad expuestas por los alumnos y se repartirá la documentación de INCIBE.

3. Algunas de las medidas imprescindibles sobre la seguridad en el tratamiento de dispositivos

1.3 Actividad 3: Seguridad en el puesto de trabajo.

Objetivos:

- Tomar conciencia de la importancia de organizar bien la información tanto digital como en papel.
- Tomar conciencia de la importancia de las contraseñas privadas y seguras como método preventivo frente a ataques informáticos.
- Aprender a crear contraseñas seguras
- Aprender a gestionar las contraseñas con ayuda de un gestor de contraseñas.

Resumen:

En esta sesión el alumno deberá aprender a tomar conciencia de la importancia de organizar bien la información diaria que maneje en su puesto de trabajo, tanto en papel como en digital y también a crearse unos protocolos seguros de utilización de contraseñas para proteger su vida digital y la de su empresa.

Metodología:

Se plantea un trabajo cooperativo con el alumnado como protagonista, para que sean ellos quienes vayan descubriendo las pautas en el uso responsable de dispositivos de almacenamiento portables. También se realizará una pequeña práctica en la que el alumno aprenderá a crear contraseñas seguras y a utilizar una sencilla aplicación de gestión de contraseñas instalada en su propio móvil.

Materiales:

- Equipo audiovisual con Internet para el grupo.
- Equipos informáticos conectados a Internet para cada participante.
- Teléfono móvil personal de cada alumno.
- Apuntes impresos para los alumnos a modo de recuerdo propiedad de INCIBE

Estructura de la sesión:

Comenzaremos la clase con la visualización de un breve vídeo que nos ayuda a concienciarnos de la importancia de proteger nuestra vida digital:

https://www.youtube.com/watch?v=xim7z4SzauI

Preguntas para guiar el debate posterior:

- ¿Cómo organizamos la información en nuestros ordenadores personales?
- ¿Qué aplicaciones tienen los alumnos protegidas mediante contraseña?
- ¿Cuántas contraseñas diferentes tenemos?
- ¿Qué tipo de contraseña utilizamos?

Teniendo en cuenta lo aprendido en las sesiones anteriores, los alumnos comienzan a decir uno por uno medidas que ellos consideran importantes para una gestión ordenada y segura de la información y también sobre el uso de contraseñas para el acceso a la misma. A medida que los alumnos avanzan en sus respuestas el profesor las irá anotando en la pizarra e irá introduciendo los contenidos y las explicaciones que desea impartir.

A continuación se visualizará el siguiente video sobre cómo crear una contraseña que sea segura y práctica al mismo tiempo:

https://www.youtube.com/watch?v=l0nnL4xr3k0

Para poner en práctica lo aprendido en el vídeo los alumnos trabajarán de forma breve en una posible contraseña personal que reúna las condiciones vistas.

A continuación se les presentará el siguiente vídeo sobre los gestores de contraseñas, para qué sirven, sus ventajas, etc.

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

Al finalizar el vídeo se invitará a los alumnos que así lo deseen a instalarse en sus dispositivos móviles la app Kee Pass (u otra de su elección que sea libre y multiplataforma). Con la ayuda del programa ITALC el profesor guiará a los alumnos tanto en su instalación como en su manejo para que comiencen a utilizarlo.

Para finalizar la sesión se realizará la puesta en común final y las conclusiones. Se realizarán los últimos retoques a las medidas de seguridad expuestas por los alumnos y se repartirá la documentación de INCIBE.

4. Algunas de las medidas imprescindibles sobre la seguridad en el puesto de trabajo.

1.4 Actividad 4: Seguridad en los dispositivos móviles y cookies.

Objetivos:

- Conocer los distintos tipos de dispositivos móviles existentes y las principales medidas para su uso seguro y responsable tanto en la vida privada como en el entorno empresarial.
- Conocer la tendencia BYOD y los riesgos que entraña.
- Concienciarse del peligro que suponen las redes WIFI públicas.
- Conocer qué son las cookies y como tratarlas.

Resumen:

En esta sesión el alumno aprenderá a utilizar de forma correcta y segura los dispositivos móviles como teléfonos, tablets, ordenadores portátiles, etc fuera del centro de trabajo o de nuestro domicilio.

Metodología:

Se plantea un trabajo cooperativo con el alumnado como protagonista, para que sean ellos quienes vayan descubriendo las pautas en el uso responsable de dispositivos electrónicos portátiles. Las explicaciones del profesor serán apoyadas por vídeos de corta duración y dinámicos.

Materiales:

- Equipo audiovisual con Internet para el grupo.
- Equipos informáticos conectados a Internet para cada participante.
- Apuntes impresos para los alumnos a modo de recuerdo propiedad de INCIBE

Estructura de la sesión:

Comenzaremos la clase con la visualización de un breve vídeo que nos ayuda a conocer cómo usar nuestros dispositivos electrónicos móviles de forma segura y responsable.

https://www.youtube.com/watch?v=HuwOrqqXz6U

Preguntas para guiar el debate posterior:

- ¿Qué tipo de dispositivos móviles utilizamos habitualmente?
- ¿Tomamos alguna medida de prevención cuando estamos fuera de casa?
- ¿Qué son las cookies y para qué sirven?

Teniendo en cuenta lo aprendido en las sesiones anteriores, los alumnos comienzan a decir uno por uno medidas que ellos consideran importantes para una gestión ordenada y segura de la información y también sobre el uso de contraseñas para el acceso a la misma. A medida que los alumnos avanzan en sus respuestas el profesor las irá anotando en la pizarra e irá introduciendo los contenidos y las explicaciones que desea impartir.

A continuación se visualizará el siguiente video sobre las cookies:

https://www.youtube.com/watch?v=WPKLBgEF-PU

Tras su visualización el profesor guiará a los alumnos a que exploren en sus ordenadores la configuración que tienen con respecto a las cookies y como cambiarla.

Para finalizar la sesión se realizará la puesta en común final y las conclusiones. Se realizarán los últimos retoques a las medidas de seguridad expuestas por los alumnos y se repartirá la documentación de INCIBE.

Si diera tiempo en esta misma sesión se realizaría el test de evaluación de los contenidos vistos en las cuatro sesiones (ver apartado siguiente).

5. Algunas de las medidas imprescindibles sobre la seguridad en dispositivos móviles.

6. **Póster motivación INCIBE.**