INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

Estudio sobre medidas de seguridad en plataformas educativas

OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN

Instituto Nacional
de Tecnologías
de la Comunicación

Edición: Julio de 2008

INTECO quiere agradecer especialmente su colaboración en la elaboración de este estudio a:

GRUPO SM

ÍNDICE

PUNTOS CLAVE

I Qué es una plataforma educativa

Pese a que existe un amplio consenso a la hora de considerar la plataforma educativa como la herramienta ideal para proporcionar un espacio para el aprendizaje, la información, la comunicación y la participación de los diferentes miembros de la comunidad educativa, no resulta fácil de definir.

Además, en paralelo surge la dificultad de categorización. Debido a la multitud de usos y funciones que tienen las plataformas, conviven a la vez y en el mismo entorno educativo plataformas desarrolladas con *software* libre y propietario.

Lo que también las diferencia son el desarrollo interno y la estructura, enfocada al funcionamiento que los distintos usuarios quieran hacer de ellas. Así, podemos distinguir entre perfiles de usuario (alumnos, docentes, padres, consejerías de educación e inspección educativa) y perfiles de proveedores de servicios.

Con independencia de estos problemas, lo que parece lógico, tal y como han puesto de manifiesto los expertos entrevistados, es que el desarrollo de las plataformas depende de garantizar al menos cuatro pilares básicos: conectividad, disponibilidad de los recursos tecnológicos y de contenidos didácticos y formación del profesorado.

II Por qué debe ser securizada una plataforma educativa

La principal particularidad de una plataforma educativa estriba en el uso masivo que los menores hacen de ella.

El futuro de la seguridad de las plataformas educativas, en opinión de los expertos, se divide entre los que consideran que el incremento de su utilización es directamente proporcional a los problemas de seguridad y los que consideran que habrá que estar alerta y adoptar una postura proactiva.

Existen diversas normas que repercuten en la seguridad de la información, tanto en el ámbito legislativo como relativas a las buenas prácticas.

III Análisis de riesgos

Ante la diversidad de amenazas que tienen o pueden tener las plataformas, es necesario realizar una estimación sobre la probabilidad de la ocurrencia de dichas amenazas y considerar los daños que causarían. Dicho análisis permite contrastar cuáles son los puntos fuertes (seguridad lógica, control de acceso, compra y desarrollo, ausencia de incidencias, concienciación y cumplimiento de la legislación) y las vulnerabilidades de las plataformas.

IV Necesidades detectadas

Como paso previo a identificar las recomendaciones, INTECO ha procedido a identificar cuáles son las necesidades para cada uno de los perfiles de las plataformas basándose en que su desarrollo sea con vistas a desarrollar y/o reestructurar una plataforma útil y segura.

El desarrollo de las necesidades se ha realizado desde diferentes ámbitos de actuación que afectarán a las plataformas, dependiendo del grado de evolución de las mismas, y que se han desarrollado en sensibilización, formación e información, normativa, certificación y estandarización, funcionalidad y seguridad de contenidos.

V Recomendaciones y propuestas

A raíz de las necesidades anteriormente identificadas, INTECO propone una serie de recomendaciones dirigidas a los diferentes actores y usuarios de las plataformas educativas y de los servicios inherentes a ellas. Se han de tener presentes estas recomendaciones a la hora de establecer los criterios para diseñar las plataformas, desarrollar y controlar los contenidos y utilidades, y usar las plataformas para que se puedan mejorar los niveles de seguridad que existen actualmente.

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Presentación

1.1.1 Instituto Nacional de Tecnologías de la Comunicación

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), sociedad estatal promovida por el Ministerio de Industria, Turismo y Comercio, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos de los ámbitos de la innovación y de la tecnología. Su objetivo es doble: por una parte, contribuir a la convergencia de España con Europa en la Sociedad de la Información, y, de otra parte, promover el desarrollo regional, enraizando en León un proyecto con vocación global.

La misión de INTECO es impulsar y desarrollar proyectos de innovación relacionados con el sector de las Tecnologías de la Información y la Comunicación (TIC), y, en general, en el ámbito de la Sociedad de la Información, que mejoren la posición de España y aporten competitividad, extendiendo sus capacidades tanto al entorno europeo como al latinoamericano.

Así, el Instituto tiene la vocación de ser un centro de desarrollo de carácter innovador y de interés público a nivel escala nacional, que constituirá una iniciativa enriquecedora y difusora de las nuevas tecnologías en España en clara sintonía con Europa.

El objeto social de INTECO es la gestión, asesoramiento, promoción y difusión de proyectos tecnológicos en el marco de la Sociedad de la Información. Para ello, INTECO desarrollará actuaciones, al menos, en líneas estratégicas de Seguridad Tecnológica, Accesibilidad, Innovación en soluciones de TIC para la PYME, e-Salud y, e-Democracia.

1.1.2 Observatorio de la Seguridad de la Información

El Observatorio de la Seguridad de la Información se inserta dentro de la línea estratégica de actuación de INTECO en materia de seguridad tecnológica. Nace con el objetivo de describir de manera detallada y sistemática el nivel de seguridad y confianza en la sociedad de la información y de generar conocimiento especializado en la materia. De este modo, se encuentra al servicio de los ciudadanos, las empresas y las administraciones públicas españolas para describir, analizar, asesorar y difundir la cultura de la seguridad de la información y la e-confianza.

El Observatorio ha diseñado un plan de actividades y estudios con el objeto de producir conocimiento especializado y útil en materia de seguridad por parte de INTECO, así como de elaborar recomendaciones y propuestas que definan tendencias válidas para la toma de decisiones futuras por parte de los poderes públicos.

Dentro de este plan de acción se realizan labores de investigación, análisis, estudio, asesoramiento y divulgación que atenderán, entre otras, a las siguientes estrategias:

- Elaboración de estudios e informes propios en materia de seguridad de las tecnologías de la información y la comunicación, con especial énfasis en la seguridad en Internet.

- Seguimiento de los principales indicadores y políticas públicas relacionados con la seguridad de la información y la confianza en los ámbitos nacional e internacional.

- Generación de una base de datos que permita el análisis y evaluación de la seguridad y la confianza con una perspectiva temporal.

- Impulso de proyectos de investigación en materia de seguridad de TIC.

- Difusión de estudios e informes publicados por otras entidades y organismos nacionales e internacionales, así como de información sobre la actualidad nacional y europea en materia de seguridad y confianza en la sociedad de la información.

- Asesoramiento a las administraciones públicas en materia de seguridad de la información y la confianza, así como el apoyo a la elaboración, seguimiento y evaluación de políticas públicas en este ámbito.

1.2 Objetivos del estudio

El presente informe se enmarca dentro del proceso de cambio tecnológico en el que está inmersa la sociedad actual y al que progresivamente se va incorporando el entorno educativo.

En concreto, la importancia que tienen las plataformas educativas como herramientas para acercar las tecnologías a la educación hace que resulte imprescindible desarrollar estudios que analicen la seguridad en estos nuevos entornos virtuales de trabajo.

Ante esta realidad emergente, INTECO se planteó la necesidad de realizar una investigación que permitiera:

- Conocer el punto de vista que tienen los desarrolladores, proveedores y usuarios de estas plataformas educativas online para niños, centrando el foco del estudio en la identificación de riesgos y soluciones de seguridad.

- Generar líneas estratégicas de actuación y mejora de la calidad de estos servicios.

- Servir de base para orientar y apoyar la toma de decisiones por parte de la Administración en materia de e-confianza y seguridad de la información.

En este sentido, el estudio tiene unos objetivos amplios que se concretan en los objetivos generales y operativos que se detallan a continuación.

Objetivos generales

1) Alcanzar una comprensión global sobre la seguridad en las plataformas educativas.

2) Identificar, mediante un proceso flexible, holístico y contextualizado, y desde las distintas perspectivas de expertos, empresas desarrolladoras de soluciones y demás implicados, las incidencias y necesidades de los usuarios respecto a las plataformas educativas online.

3) Definir unas recomendaciones generales sobre normativa, buenas prácticas y pautas de seguridad en relación con el uso y el desarrollo de estas plataformas.

Objetivos operativos

1) Obtener información general sobre las plataformas educativas: su conceptualización, funcionalidades, usuarios, etc.

2) Establecer una tipología de las plataformas educativas existentes en la actualidad y definir algunas de sus características.

3) Conocer el nivel de seguridad con el que se trabaja desde los distintos proveedores y desarrolladores de plataformas, y compararlo con el que se considerada óptimo.

4) Detectar los principales riesgos en materia de seguridad, así como las posibles soluciones a implementar.

1.3 Diseño metodológico

A continuación, se describe el proceso metodológico empleado en la elaboración del estudio.

Fase de investigación

La metodología empleada en esta fase consta de tres etapas:

- **Búsqueda y análisis documental,** donde se han considerado numerosos estudios y artículos de los ámbitos nacional e internacional.

- Realización de **29 entrevistas semiestructuradas**[1] **con detenimiento** y **20 cuestionarios autoaplicados** con expertos y agentes clave que cuentan con experiencias de éxito en seguridad de plataformas educativas online, y con amplios conocimientos en el sector. Estas entrevistas han sido distribuidas entre los siguientes perfiles[2]:
    - Administración Pública española (Ministerio de Educación y Ciencia; Ministerio de Industria, Turismo y Comercio, y consejerías de educación autonómicas).
    - Empresas especializadas en el desarrollo tecnológico de plataformas educativas y/o de soluciones de seguridad para ellas en los ámbitos nacional e internacional.
    - Expertos en seguridad informática.
    - Fuerzas y Cuerpos de Seguridad del Estado especializados en delitos telemáticos.
    - Asociaciones dedicadas a la protección del menor ante situaciones de riesgo en Internet.
    - Usuarios de las plataformas educativas: profesores, padres y asociaciones que los representan.
- Realización de un **foro de discusión con un grupo de alumnos** de Secundaria y Bachillerato de diferentes edades, sexos y niveles de competencia tecnológica.

Fase de análisis y debate de las conclusiones

Paralelamente, se llevaron a cabo reuniones con el objetivo de consolidar la información obtenida en la fase anterior, tratando de hacer un primer análisis y clasificación tanto de las fuentes documentales como de la información obtenida de las entrevistas.

Para ello, con anterioridad a la redacción del informe, se mantuvieron varias reuniones de equipo en las que se elaboró el índice de contenidos, hasta llegar a su validación y planteamiento definitivo.

Fase de recomendaciones de actuación

[1] Consiste en un proceso de comunicación dinámica entre dos personas, entrevistador y entrevistado, bajo el control del primero. El objetivo que persigue es obtener información lo más implicadora posible sobre el objeto de análisis que se plantea.

[2] En el anexo I se muestra una relación de todas las entidades y profesionales que han sido entrevistados durante la fase de investigación.

Sobre la base de datos de este último informe, se identificaron las recomendaciones y orientaciones de actuación expuestas por los propios expertos entrevistados, con el objeto de establecer los posibles alcances y responsabilidades los ámbitos de la autorregulación, la legislación, la certificación y la estandarización necesarias para la creación y/o desarrollo de las plataformas; la sensibilización, la formación y la información de los usuarios, y, en general, otras medidas que desarrollarán las entidades públicas.

2 QUÉ ES UNA PLATAFORMA EDUCATIVA

La evolución de las plataformas educativas se muestra muy ligada al desarrollo de la sociedad de la información y del conocimiento, y, más en concreto, al de los sistemas educativos, que tienden, progresivamente, a adaptarse a las necesidades reales del mundo laboral.

La alfabetización se reconoce ahora como un concepto cambiante en el tiempo, donde adquiere mayor relevancia el dominio de los procesos y estrategias cognitivas que la asimilación de contenidos, y en donde ya no existen barreras espacio-temporales que limiten los aprendizajes.

En este marco de innovación y cambio, la opción de generar entornos virtuales de aprendizaje basados en las Tecnologías de la Información y la Comunicación (TIC), supone responder de forma integral a los requerimientos que impone la Sociedad del Conocimiento y a las nuevas necesidades del entorno educativo. Es dentro de este contexto de innovación donde surgen las plataformas educativas.

2.1 Las tecnologías de la información y la comunicación en la educación

La incorporación de las TIC a la educación ha venido marcada, tradicionalmente, más por la tecnología que por la pedagogía y la didáctica. En la escuela, al igual que en otros ámbitos, el uso creciente de las tecnologías ha estado dictado por su evolución y desarrollo, y, aunque se han aplicado a la educación desde mucho tiempo atrás, es a partir de los años ochenta cuando comienza su generalización.

La aparición de los ordenadores personales a principios de los años ochenta y el acceso a redes de telecomunicaciones especializadas gracias a Internet hicieron posible el intercambio y acceso mundial a fuentes de información, generando con ello importantes cambios en el ámbito educativo.

Desde los años noventa hasta la actualidad, se han ido incorporando nuevos recursos tecnológicos que ponen de manifiesto la necesidad de reconceptualizar los procesos y modelos tradicionales de enseñanza y aprendizaje.

En la actualidad, resulta impensable abandonar a los jóvenes en la cultura global de la comunicación sin formarlos acerca de cuándo, cómo y por qué usar las tecnologías emergentes. El desarrollo de conceptos como “aprendizaje a lo largo de toda la vida”, “aprender a aprender”, etc., han supuesto que la institución escolar deba modificar los roles tradicionales del profesor y del alumno, y que, en muchos casos, comiencen ya a concretarse en criterios estandarizados y generales.

En España, la Ley Orgánica de Educación (LOE) y los reales decretos de desarrollo de las enseñanzas mínimas[3] establecen la alfabetización tecnológica como una de las competencias básicas que deben adquirir los alumnos. De igual modo, la UNESCO acaba de publicar los *Estándares de competencia en TIC para docentes*[4], con el fin de que cada país se guíe por tales normas para maximizar la formación de los profesores en materias de índole tecnológica.

La entidad pública empresarial Red.es, dependiente del Ministerio de Industria, Turismo y Comercio, junto con el Ministerio de Educación y Ciencia y las distintas administraciones educativas autonómicas, ha lanzado diferentes programas dirigidos a potenciar la incorporación y uso de la tecnología en los centros públicos españoles no universitarios.

Concretamente, se han impulsado los programas Internet en la Escuela (2002-2006), Internet en el Aula[5] (2005-2008) y Enseña[6] (2007-2008), que están dirigidos a reforzar y complementar las políticas de fomento del desarrollo no discriminatorio de la sociedad de la información en el entorno educativo, buscando la cohesión territorial y que se compartan iniciativas entre todas las comunidades autónomas participantes.

2.2 Problemas de categorización

Pese a que existe un amplio consenso a la hora de considerar la plataforma educativa como la herramienta ideal para proporcionar un espacio para el aprendizaje, la información, la comunicación y la participación de los diferentes miembros de la comunidad educativa, no resulta fácil de definir.

Atendiendo a las distintas explicaciones recogidas en las entrevistas[7], se pueden destacar algunos puntos recurrentes que permiten la configuración de diferentes acepciones:

- Aquellos que, a partir de su origen y evolución, afirman que su comienzo se remonta al de las plataformas de *e-learning*, pasando con el tiempo a proporcionar más servicios, de manera que estas plataformas pueden ser consideradas como una concreción del esfuerzo que en los últimos años está haciendo la comunidad educativa por buscar fórmulas de renovación de los procesos de enseñanza-aprendizaje.

[3] Real Decreto 1631/2006, de 29 de diciembre, por el que se establecen las enseñanzas mínimas correspondientes a la Educación Secundaria Obligatoria, BOE de 5 de enero de 2007.

[4] Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) (2008): *Estándares de competencia en TIC para docentes*. En línea. Disponible en http://cst.unesco-ci.org/sites/projects/cst/default.aspx

[5] [Homepage]. Consultado el día 3 de abril de 2008 en la World Wide Web: http://www.red.es/actividades/Internet_aula.html

[6] [Homepage]. Consultado el día 3 de abril de 2008 en la World Wide Web: http://www.red.es/actividades/ensena.html

[7] No ha sido posible clasificar por perfil profesional a los entrevistados que han participado en la fase de trabajo de campo.

- Otros destacan, en su definición, el valor que tienen como sistemas de información de los centros educativos, y, más en concreto, como un servicio que gestiona un centro para relacionarse, por medio de Internet, con la comunidad educativa.

- Desde el punto de vista de sus funcionalidades, se las conceptualiza como aplicaciones que permiten gestionar procesos de enseñanza-aprendizaje o cursos de carácter virtual o semipresencial, así como llevar a cabo todas las funciones de gestión académica y administrativa.

- Una última acepción del término, mucho más general, admitiría como plataforma educativa cualquier portal de la Administración educativa o del centro escolar: de contenidos online, de gestión académica, de servicios educativos (videoconferencia, bibliotecas online, etc.), páginas y *blogs* educativos, etc.

En cualquier caso, el denominador común parece definirlas como una **herramienta cuyo diseño y finalidad principal es dar respuesta de forma integral a las múltiples necesidades inherentes a la vida de un centro educativo**. Se considera, incluso, que se trata de una cuestión de organización escolar a la que puede dar cobertura la tecnología.

2.2.1 Estructura y funcionamiento general de una plataforma educativa

Las plataformas educativas tienen, normalmente, una estructura modular que hace posible su adaptación a la realidad de los diferentes centros escolares.

Cuentan, estructuralmente, con distintos módulos que permiten responder a las necesidades de gestión de los centros a tres grandes niveles: gestión administrativa y académica, gestión de la comunicación y gestión del proceso de enseñanza-aprendizaje.

Para ello, estos sistemas tecnológicos proporcionan a los usuarios espacios de trabajo compartidos destinados al intercambio de contenidos e información, incorporan herramientas de comunicación (*chats*, correos, foros de debate, videoconferencias, *blogs*, etc.) y, en muchos casos, cuentan con un gran repositorio de objetos digitales de aprendizaje desarrollados por terceros, así como con herramientas propias para la generación de recursos.

El funcionamiento de las plataformas se orienta a dar servicio a cuatro perfiles de usuario: administradores de centro, padres, alumnos y profesores. Cada uno de estos perfiles está identificado mediante un nombre de usuario y una contraseña, a través de los cuales se accede a la plataforma. Esta estructura de funcionamiento supone la creación de un espacio de trabajo e interacción cerrado y controlado, en el que las situaciones de riesgo que pueden vivir los usuarios tienen una menor intensidad que fuera de los mismos.

2.2.2 Funciones que desempeñan estas plataformas

Una plataforma de aprendizaje tiene, conjuntamente, *hardware*[8], *software*[9] y servicios de apoyo para permitir modos más efectivos de trabajo, tanto fuera como dentro del aula.

Aunque pueden variar considerablemente en su diseño y desarrollo, siempre deben proporcionar una serie de funcionalidades –como, por ejemplo, herramientas colaborativas que estimulen la idea de cooperación e interacción– y medios para el desarrollo de nuevos métodos de trabajo y modelos educativos que vayan más allá del simple uso de la tecnología como herramienta.

Si analizamos las principales funcionalidades que se definen en su diseño, encontramos, fundamentalmente, dos aplicaciones:

1) Educación a distancia, cuando el proceso educativo no es presencial.

2) Apoyo y complemento de la educación presencial.

Recientemente, las plataformas educativas se utilizan también para generar espacios de discusión y construcción de conocimiento por parte de grupos de investigación, o para la implementación de comunidades virtuales y redes de aprendizaje, por parte de grupos de personas unidos en torno a una temática de interés.

Atendiendo a sus funciones como apoyo al proceso de enseñanza-aprendizaje, algunas de las más destacadas están relacionadas con:

- La alfabetización digital de los estudiantes, así como de los profesores y las familias.
- El acceso a la información, comunicación, gestión y procesamiento de datos.
- La gestión académico-administrativa del centro: secretaría, biblioteca, etc.
- El uso didáctico para facilitar los procesos de enseñanza-aprendizaje.
- La comunicación con las familias y con el entorno.
- La relación entre profesores a través de redes y comunidades virtuales: compartir recursos, experiencias, etc.

[8] *Hardware:* cualquier componente físico utilizado para que funcione la plataforma (servidores, discos duros, sistemas de alimentación ininterrumpida, balanceadores, *firewalls*, etc.)

[9] *Software:* conjunto del código de programación que hace posible la realización de una tarea específica.

Un análisis más general permite que estas también puedan ser concebidas y conceptualizadas como:

- Medio de expresión y creación multimedia para escribir, dibujar, realizar presentaciones multimedia, elaborar páginas web, etc.
- Espacio generador y soporte de nuevos espacios formativos.
- Canal de comunicación que facilita la comunicación interpersonal, y el intercambio de ideas y materiales en un entorno colaborativo.
- Fuente abierta de información y de recursos.
- Instrumento cognitivo que apoya procesos de construcción del conocimiento.
- Instrumento para la gestión administrativa y tutorial.
- Herramienta para la orientación, el diagnóstico y el seguimiento de estudiantes.
- Instrumento didáctico y para la evaluación que proporciona una corrección rápida y *feedback* inmediato, una reducción de tiempos y costes, la posibilidad de seguir el "rastro" del alumno, etc.

2.2.3 Tipos de plataformas encontradas

En la actualidad, existe un número importante de plataformas educativas disponibles. Algunas son productos comerciales con un coste asociado, mientras que otras son herramientas gratuitas que suelen estar desarrolladas en código abierto, lo que permite modificar o adaptar, mediante programación, los distintos módulos que las componen.

Atendiendo al periodo de tiempo en que estas plataformas han cobrado importancia, cabe esperar que su proliferación y perfeccionamiento vayan creciendo a un ritmo considerable y en un corto plazo de tiempo. Esto es válido tanto para las plataformas que han nacido por iniciativa de las diferentes consejerías de educación, como para aquellas que lo han hecho por iniciativa de empresas privadas.

Plataformas-portales de las consejerías de educación

Durante los últimos años, cada una de las comunidades autónomas ha estado realizando importantes inversiones para dotar a sus centros escolares de recursos y herramientas tecnológicos. De forma simultánea a este esfuerzo, se está poniendo énfasis en la alfabetización digital de todos los miembros de la comunidad educativa.

Todas las consejerías de educación están trabajando con el objetivo de proporcionar a los centros docentes conectividad de banda ancha y extender las redes educativas intra e

intercentros, así como en la dotación e incorporación de nuevos recursos tecnológicos y de espacios comunes en Internet, a través del desarrollo de estas plataformas educativas.

Pese a la indudable importancia que tiene dotar a los centros con los medios tecnológicos necesarios, las opiniones recogidas en las entrevistas realizadas a los agentes clave ponen de manifiesto que son los docentes los responsables últimos de su utilización pedagógica en el aula. Así lo corroboran los resultados arrojados por un estudio llevado a cabo por Red.es y el Centro Nacional de Información y Comunicación Educativa (CNICE)[10]. Sobre una muestra de unos 20.000 profesores, los datos revelan que las principales barreras citadas para una mayor utilización se relacionan, de una u otra manera, con la figura del profesor, y son: i) falta de formación en TIC y en la plataforma, ii) falta de tiempo para aprender, iii) falta de apoyo dentro del centro y iv) falta de herramientas.

Esta realidad ha sido comprendida por las distintas consejerías que están llevando a cabo importantes y variadas iniciativas de formación para el profesorado, así como diferentes proyectos y concursos que animan a los docentes a crear recursos que después puedan ser compartidos en repositorios comunes.

Por otro lado, una revisión con detenimiento de las plataformas educativas existentes en el panorama nacional, cuya realización ha sido impulsada por las administraciones educativas, nos muestra que existe una cierta tendencia al uso del *software* libre en su desarrollo. En todas ellas son similares la lógica de acceso y sus funcionalidades, y, en general, las opiniones de los desarrolladores reflejan que la seguridad es adecuada con el grado de uso de las mismas.

Iniciativas privadas

También existen en el mercado varias plataformas desarrolladas por empresas privadas. Sus funcionalidades están orientadas a apoyar la enseñanza reglada, intentando innovar y mejorar los procesos de enseñanza-aprendizaje. Además, proporcionan a los centros eficientes herramientas de gestión académica y administrativa, y se constituyen en potentes canales que favorecen la comunicación y el intercambio de información entre los diferentes agentes del mundo educativo. En este caso, las aplicaciones han sido desarrolladas, normalmente, en *software* propietario.

Desde hace poco tiempo, se está observando una gran proliferación de soluciones orientadas a facilitar la comunicación familia-colegio. Sin embargo, resulta más difícil

[10] Red.es y Centro Nacional de Información y Comunicación Educativa (CNICE) (2007): *Informe sobre la implantación y uso de las TIC en los centros docentes de Educación Primaria y Secundaria (curso 2005-2006)*. Madrid. En línea. Disponible en http://www.oei.es/TIC/DocumentoBasico.pdf

encontrar plataformas que integren contenidos digitales que se adapten al currículo de los alumnos.

2.2.4 Plataforma ideal: gestión académica y administrativa, contenidos digitales y comunicación

A la hora de definir lo que podría entenderse como una plataforma educativa completa, existe un consenso generalizado en que la plataforma ideal debe permitir gestionar conjuntamente todas las necesidades de un centro educativo asociadas a labores de tipo administrativo y académico, la comunicación entre los diferentes miembros de la comunidad educativa y el apoyo a la docencia.

Se constata que existen muy pocas plataformas que implementen las tres funcionalidades. El módulo de comunicación es, en este momento, el más demandado por los centros, y el menos desarrollado es el correspondiente a los contenidos. De una u otra forma, todos los centros tienen alguna herramienta que facilita la gestión administrativa y académica.

Es también reseñable que la mayoría de los entrevistados hayan puesto de manifiesto que, para sacar todo el partido a estas plataformas, es necesario atender y garantizar cuatro pilares básicos: conectividad, disponibilidad de recursos tecnológicos, y de contenidos didácticos y formación del profesorado.

Siendo indudables las enormes potencialidades derivadas de contar con plataformas que gestionen de forma integrada todas las acciones antes descritas, no hay que olvidar que, acompañando al desarrollo de nuevas funcionalidades, pueden verse también incrementados los riesgos de seguridad (dado que cada vez contendrán datos de mayor sensibilidad).

En este punto, las opiniones de los expertos se dividen nuevamente entre los que no ven que el futuro se asocie a una mayor problemática en seguridad y los que consideran que habrá que estar alerta y adoptar una postura proactiva, no esperando a que sean las incidencias las que nos hagan conscientes de la necesidad de generar sistemas más seguros. En lo que sí coinciden ambos grupos es en señalar que un incidente serio de seguridad dañaría la credibilidad de estas herramientas y frenaría el desarrollo del sector.

2.3 Perfiles de los usuarios

Hasta hace poco tiempo, la utilización de plataformas educativas normalmente quedaba relegada a centros con una larga trayectoria en TIC, a profesores que las empleaban para su formación y a entornos universitarios. Pero esta realidad está cambiando. En la actualidad, se reconoce que se trata de una potente herramienta de la que se pueden beneficiar todos los miembros de la comunidad educativa.

La incorporación y uso de dichas plataformas en el ámbito de la educación no se ha producido en todos los sectores por igual. Atendiendo a las estadísticas generales de uso de las TIC[11], comprobamos que se utilizan más en el sector público que en el privado, y más en Secundaria que en Primaria. Estos datos se repiten también en países como el Reino Unido, donde, además, los datos reflejan que existe cierta resistencia entre el profesorado para integrar los adelantos tecnológicos en las dinámicas de aula. Concretamente, se calcula que aproximadamente un 20% de los profesores utiliza habitualmente las plataformas y un 40% las usa esporádicamente[12].

En cualquier caso, lo comúnmente aceptado es que una plataforma de aprendizaje que se incorpore a las prácticas de trabajo de la escuela puede ofrecer un amplio rango de beneficios a los profesores, alumnos y padres, y, al mismo tiempo, apoyar los procesos de organización y gestión del centro.

2.3.1 Alumnos

Constituyen una generación que ha nacido con la tecnología. En su mayoría, tienen en común el gusto por las TIC, y son usuarios activos de plataformas educativas tanto en el ámbito escolar como en el particular, en su tiempo libre.

El uso principal que hacen de estos recursos es para jugar, comunicarse (mensajería instantánea, *chats*, foros, *e-mails*, etc.) y, desde hace poco tiempo, como herramienta de trabajo. Todavía tienen fuertemente asociado el concepto de tecnología con el de juego, quizá porque en sus comienzos esta fue su finalidad. En la actualidad, empiezan a tomar conciencia de su valor como apoyo en sus aprendizajes, algo a lo que contribuye también la incorporación de estas plataformas en los procesos de enseñanza-aprendizaje.

Por otro lado, tanto en las opiniones recogidas de los expertos sobre el uso que los niños y jóvenes hacen de la tecnología como en los estudios revisados se ponen de manifiesto las diferencias existentes en la utilización que hacen de Internet en función del sexo: los chicos prefieren juegos online principalmente, mientras que las chicas tienden más a páginas de comunicación, de interacción[13], etc.

Las impresiones recogidas muestran que el alumnado, en muchos casos, es autodidacta de las tecnologías, al ir un paso por delante de sus profesores y padres, que, por diferencias generacionales, no han tenido estas experiencias ni formación. Esto hace que, en materia de seguridad, la información que reciben provenga, en su mayoría, de las experiencias de sus compañeros y de su propio sentido común.

---

[11] Red.es y Centro Nacional de Información y Comunicación Educativa (CNICE): óp. cit.,10.

[12] [Homepage]. Consultado el día 3 de abril de 2008 en la World Wide Web: www.becta.org.uk/research

[13] APCI y Protégeles (2002): *Seguridad infantil y costumbres de los menores en Internet*. En línea. Madrid: El Defensor del Menor en la Comunidad de Madrid. Disponible en http://www.protegeles.com/costumbres.asp

Un estudio[14] llevado a cabo por la Asociación Protégeles pone de manifiesto que los menores de ambos sexos están igualmente desinformados sobre las normas de seguridad básicas para navegar por Internet: 55%, ellas, y 53%, ellos.

2.3.2 Profesores

El perfil más habitual del profesor responde al de un profesional que se ha formado en un contexto en el que las TIC no existían o bien se integraban en la dinámica del aula como un elemento de apoyo a la explicación del docente. Para los más jóvenes, la informática ha sido una materia más del currículo oficial que se enseñaba como una asignatura independiente.

Esta experiencia personal, unida al hecho de que la mayoría de los docentes tampoco han recibido formación específica sobre cómo integrar las TIC en el aula durante sus estudios universitarios, tiene como consecuencia fundamental que, en general, este colectivo profesional tenga escasos conocimientos teóricos y experiencia práctica sobre la forma de implementarlas de manera eficaz en su quehacer cotidiano[15].

Las opiniones revelan que, como usuarios de las plataformas, las utilizan principalmente como recurso educativo, para trabajar con sus alumnos en clase y, a nivel particular, para su formación personal.

En los últimos años, sin embargo, son tales el auge y la necesidad de incorporar las tecnologías en los procesos de enseñanza-aprendizaje, que la mayoría de las consejerías de educación han creado la figura del coordinador TIC. El docente que asume esta responsabilidad en cada centro está liberado de un porcentaje de sus horas lectivas para poder dinamizar y liderar estos procesos entre sus compañeros. Algunas de sus principales funciones son:

- Coordinar y dinamizar la integración curricular de las tecnologías de la información y la comunicación.
- Elaborar propuestas para la organización y gestión de los medios y recursos tecnológicos, así como velar por su cumplimiento.
- Asesorar al profesorado sobre materiales curriculares en soportes multimedia, en su utilización y en la estrategia de incorporación a la planificación didáctica.
- Realizar el análisis de necesidades del centro relacionadas con las TIC.

[14] APCI y PROTÉGELES, op. cit.,13.

[15] Sigales, C. (2004): *Formación universitaria y TIC: nuevos usos y nuevos roles*. En línea. Disponible en http://www.uoc.edu/rusc/dt/esp/sigales0704.pdf

- Colaborar con las estructuras de coordinación del ámbito de las TIC que se establezcan, a fin de garantizar actuaciones coherentes del centro, y poder incorporar y difundir iniciativas exitosas.

- Supervisar la instalación, configuración y desinstalación del *software* de finalidad curricular.

- Gestionar la red: altas y bajas de usuarios, gestión de permisos, resolución de pequeñas incidencias, etc.

Resulta innegable, desde todas las perspectivas, que un elemento clave para la incorporación de las plataformas y para el cambio metodológico es sin duda el profesor. En la actualidad, desde las diferentes administraciones educativas, se está haciendo una clara apuesta por ellos en lo referente a la dotación de recursos y la formación.

2.3.3 Padres

Al analizar el perfil de los padres como usuarios de las tecnologías en general y, más en concreto, de las plataformas educativas, se encuentran varios puntos que hay que destacar.

En primer lugar, la práctica totalidad de las opiniones recogidas de asociaciones, expertos en seguridad y administraciones educativas los describe como grandes desconocedores de las TIC, lo que conlleva que, en la mayor parte de los casos, no puedan controlar lo que hacen sus hijos frente al ordenador. A pesar de que juegan un papel fundamental a la hora de prevenir a sus hijos sobre situaciones de riesgo, la realidad es que sus actuaciones suelen limitarse a prohibirles que vean contenidos sexuales o violentos en la televisión, sin ser conscientes de lo que ven o a lo que se exponen mientras navegan en Internet.

Por otro lado, como usuarios de plataformas, la mayoría afirman utilizarlas como medio de comunicación que les permite participar en el proceso de enseñanza-aprendizaje de sus hijos. Sin embargo, reconocen que todavía el grado de implicación y uso está lejos de ser el óptimo y adecuado.

Todos estos aspectos ponen de manifiesto la necesidad de que los padres reciban formación orientada a sensibilizarlos sobre los problemas de seguridad, ya que, en estos temas, una pieza clave reside en la concienciación de las familias. En esta línea, se observa que los padres están demandando entornos en los que sus hijos puedan jugar y aprender de forma autónoma y segura, pero sin estar expuestos a la inmensidad de Internet. Las plataformas educativas comienzan a ser estos espacios virtuales de aprendizaje e interacción demandados.

2.3.4 Consejerías de educación e inspección educativa

Otro posible perfil de usuario que puede descubrir múltiples funcionalidades en las plataformas educativas, en la medida en que necesitan para su trabajo datos reales de tipo académico de los alumnos matriculados en un determinado centro, son las administraciones públicas que tengan competencias sobre temas educativos y, más en concreto, la inspección educativa. Con mucha frecuencia, tienen que pedir información a los centros para poder conocer la realidad y tomar decisiones en asuntos como los procesos de matriculación, la escolarización, la concesión de becas, las estadísticas de resultados, etc. Todas estas solicitudes de información suelen ser un trastorno para la dinámica normal de funcionamiento de los centros y exigen un esfuerzo administrativo extra.

La utilización de plataformas educativas que gestionen de forma integral toda la información administrativa y académica de los alumnos y el establecimiento de estándares de intercambio de datos redundarían en una descarga de trabajo para los propios centros, y harían mucho más ágiles la toma de decisiones y los procesos internos de gestión de las autoridades educativas.

2.4 Perfiles de los proveedores de servicios

2.4.1 Administraciones públicas

En los últimos años, desde la Administración pública se ha hecho una clara apuesta por lograr incorporar las TIC al sector educativo. Para ello, se están llevando a cabo diferentes iniciativas y acciones, tales como dotaciones de equipamiento a los centros y/o mejoras en las infraestructuras, el desarrollo de portales educativos- plataformas, la creación de diversos organismos que trabajan para promover la incorporación de estos recursos en la educación, la organización de cursos de formación del profesorado o el desarrollo de contenidos digitales multimedia, etc.

Se pretende que el uso de Internet se produzca como vía de intercomunicación de los miembros de la comunidad escolar, como medio de acceso a un gran banco de recursos específicos de un área o asignatura, como puerta de entrada a espacios de trabajo colaborativos que, en algunos casos, extiendan el aula más allá de los espacios físicos delimitados por el centro escolar.

Como fruto de todo este esfuerzo, han ido desarrollando plataformas que responden a las necesidades de los miembros de la comunidad educativa. Actualmente, el panorama español muestra una realidad muy plural. Las diferencias son múltiples y apuntan a las funcionalidades y servicios que ofrecen, a las tecnologías de desarrollo y al grado de interdependencia de los módulos que las componen.

Los temas de seguridad en estas plataformas, en líneas generales, no son cuestiones que generen preocupación, ya que el nivel de incidencias es casi nulo y, además, es una responsabilidad que en la mayoría de las ocasiones se ha garantizado con la contratación de personal especializado externo. Consideran que las iniciativas que se están tomando responden a las necesidades de los desarrollos que hay actualmente en funcionamiento, y que, en cualquier caso, están garantizando entornos de trabajo con un nivel de riesgo muy bajo.

2.4.2 Empresas privadas

Dentro del sector privado, durante los últimos años, están apareciendo multitud de empresas orientadas a proponer soluciones tecnológicas para las necesidades del mundo educativo. Las principales empresas con intereses en la integración de las TIC, además de las de mobiliario e instalaciones, son las siguientes:

- **Las distribuidoras de *hardware* de uso general** (sistemas de redes, ordenadores, *tablets* PC, impresoras, los PDA, etc.).
- **Las distribuidoras de *hardware* orientado a los entornos formativos-comunicativos** (videoproyectores, pizarras digitales interactivas fijas y portátiles, etc.).
- **Las proveedoras de servicios de telefonía**.
- **Las proveedoras de servicios de Internet**. Diversas empresas ofrecen servicios de acceso a Internet: *hosting*[16], *housing*[17], etc.
- **Las desarrolladoras de *software* de uso general** (sistemas operativos, *software* de aplicación, etc.) En estos momentos, hay una **fuerte pugna entre los desarrollos realizados** con *software* propietario[18] y libre[19].
- **Las desarrolladoras de *software* educativo.** Además de las empresas especializadas, muchas editoriales de libros de texto han creado un departamento de desarrollos y contenidos digitales. Elaboran programas para la gestión de

[16] *Hosting:* es un servicio que provee a los usuarios de Internet de un sistema para poder almacenar información, imágenes, vídeo o cualquier contenido accesible por medio de la web.

[17] *Housing:* es un servicio consistente en alquilar un espacio físico de un centro de datos para que el cliente coloque ahí su propio ordenador. La empresa le proporciona la conexión a internet, pero el servidor lo elige el cliente, incluso el *hardware*. Es una modalidad de alojamiento web destinada, principalmente, a grandes empresas y a empresas de servicios web.

[18] *Software* propietario: es aquel tipo de *software* cuya propiedad absoluta permanece en manos de quien tiene sus derechos y no del usuario, que únicamente puede utilizarlo bajo ciertas condiciones.

[19] *Software* libre: es aquel tipo de *software* que tiene el código fuente abierto, lo que permite al usuario ejecutarlo con cualquier propósito, estudiar cómo funciona y adaptarlo a sus necesidades, así como distribuir copias, mejorarlo y liberar esas mejoras al público.

centros, plataformas de e-centro, materiales didácticos multimedia y, en algunos casos, plataformas de contenidos en red.

En la actualidad, se está observando una tendencia a la agrupación de diferentes compañías con objeto de proporcionar a las instituciones educativas soluciones integrales a sus necesidades. Esto ha hecho que existan ya en el mercado los primeros desarrollos de plataformas que responden a las tres grandes necesidades de los centros (gestión académica y administrativa, comunicación y apoyo a los procesos de enseñanza-aprendizaje[20]).

En relación con los temas de seguridad, de nuevo, la idea comúnmente recogida es que habrá que prestar mayor atención a este aspecto según se vayan incrementando las funcionalidades y las plataformas gestionen información más sensible: solicitudes de becas, datos bancarios, informes de tipo psicopedagógico, etc.

2.5 Beneficios asociados al uso de las plataformas educativas

A pesar del innegable impacto social de las TIC, todavía no contamos con unas pautas definitivas sobre cómo integrarlas en cada nivel educativo[21]. Es cierto que, en general, su utilización en los centros escolares ha ido aumentando, como lo muestran numerosos indicadores cuantitativos[22] –hay más ordenadores en las aulas y más conexiones a Internet, y los alumnos emplean esta tecnología en clase durante más tiempo–, pero no está cuantificado el rendimiento educativo asociado al uso de los medios técnicos.

La mayoría de las investigaciones llevadas a cabo sobre el impacto de las TIC en la enseñanza destacan, como paso principal, la necesidad de contar con modelos teóricos que orienten su utilización.

2.5.1 Desarrollo de un nuevo modelo pedagógico

En el proceso de incorporación del ordenador al aula, las TIC pueden ayudar a los profesores a reforzar su didáctica y práctica educativa o a transformarla. Se pueden distinguir, en síntesis, dos modelos o concepciones alternativas de la enseñanza: el modelo transmisivo y el modelo constructivista.

- **Modelo transmisivo.** El objetivo de la educación es que el alumno aprenda unos contenidos ya establecidos, sobre los que luego tendrá que rendir cuentas en un examen de evaluación. En este modelo, las TIC sirven de ayuda en el proceso,

[20] Más información, disponible en *Epígrafe 2.2.1: estructura y funcionamiento general de una plataforma educativa*.

[21] Newhouse, P. (2002): *Literature review. The impact of ICT on learning and teaching*. Western Australia, Specialist Educational Services.

[22] Red.es y Centro Nacional de Información y Comunicación Educativa (CNICE), óp. cit.,10.

contribuyendo a que el alumno amplíe la información, realice ejercicios o establezca alguna relación interactiva[23].

- **Modelo constructivista.** Basado en la concepción constructivista del aprendizaje, cuya raíz se sitúa en autores como Dewey, Bruner, Piaget o Vigotsky. Pone el énfasis principal en la actividad mental constructiva del alumno y en sus procesos de descubrimiento (Marchesi y Martín, 2003). Desde este enfoque, el objetivo es aprender con la tecnología, no sobre la tecnología. Los programas empleados buscan acomodarse al funcionamiento cognitivo del alumno, además de facilitar su actividad autónoma[24].

Una plena incorporación de la tecnología conllevaría el desarrollo de nuevos modelos pedagógicos que exigen modificar los roles del profesor y del alumno. Algunas de sus principales características son:

- **Centralidad del alumno.** El profesor debe dejar de ser un instructor que domina los conocimientos para convertirse en un facilitador y mediador del proceso de enseñanza-aprendizaje, de tal modo que el alumno sea capaz de llegar a alcanzar conocimientos por sí mismo. Es decir, se produce una evolución desde un esquema pedagógico basado en la mera transmisión del conocimiento a otro en el cual el alumno profundiza en la información facilitada por el docente a través de trabajos personales o en grupo.

  Por otra parte, la sociedad actual va a exigir al alumno ser un usuario inteligente y crítico con la multitud de información que tendrá que gestionar. Para lograr este objetivo, necesita adquirir nuevas habilidades, que en la actualidad han sido denominadas “competencias”.

- **Desarrollo de competencias.** Siguiendo las propuestas de la Unión Europea, la publicación de los Reales Decretos de Desarrollo de las Enseñanzas Mínimas de la Ley Orgánica de Educación ha supuesto la inclusión de las competencias básicas en el currículo oficial.

  Esta inclusión tiene varias finalidades: i) integrar los aprendizajes, tanto los formales –los propios de las áreas curriculares y las asignaturas– como los informales y los no formales; ii) favorecer los contextos en los que los alumnos puedan integrar sus aprendizajes, ponerlos en relación con distintos contenidos, y utilizarlos de manera eficaz para resolver problemas en diferentes situaciones y

[23] Marchesi y Martín (2003): *Tecnología y aprendizaje. Investigación sobre el impacto del ordenador en el aula*. Grupo SM.

[24] Lajoie (2002): *Computers as cognitive tools*. Hillsdale, Erbaulm.

contextos, y iii) orientar la enseñanza e inspirar las decisiones relativas a los procesos de enseñanza y aprendizaje.

Una de estas competencias cuya adquisición debe ser un logro al finalizar la Educación Secundaria Obligatoria es el tratamiento de la información y la capacidad digital. Esto implica que el alumno logre ser una persona autónoma, eficaz, responsable, crítica y reflexiva al seleccionar, tratar y utilizar la información y los soportes, así como lograr una actitud crítica y reflexiva en la valoración de la información disponible.

- **Individualización del proceso docente.** Con la incorporación de las TIC, una de las finalidades principales que se persiguen es dar solución real a la diversidad y heterogeneidad del aula. Su utilización permite adaptar la enseñanza al ritmo de aprendizaje de cada alumno, así como llevar un seguimiento personalizado de su evolución.

  El perfil profesional del docente incluye, también hoy, competencias para conocer las capacidades de sus alumnos, diseñar intervenciones centradas en la actividad y participación de estos, evaluar recursos y materiales, y, a ser posible, crear sus propios medios didácticos o, al menos, adaptar los existentes desde la perspectiva de la diversidad real de su alumnado.

- **Aprender a aprender, formación para toda la vida**[25]. Existe un consenso generalizado acerca de la importancia de utilizar las tecnologías como herramientas que permitan un cambio en la propia concepción de la educación, donde la estrategia clave para el aprendizaje sea “aprender a aprender”.

  “La persona formada no lo será a base de conocimientos inamovibles que posea en su mente, sino en función de sus capacidades para conocer lo que precise en cualquier momento..., un analfabeto será aquel que no sepa dónde ir a buscar la información que requiera, en un momento dado, para resolver una problemática concreta” (Colom).

- **Mayor implicación de las familias en los procesos de enseñanza-aprendizaje.** Otra de las grandes ventajas de las plataformas educativas consiste en que, gracias a los módulos de comunicación, se facilita el seguimiento de las familias sobre los procesos de aprendizaje de sus hijos.

[25] Marchesi y Martín (2003): óp. cit.,23.

2.5.2 Optimización de procesos de gestión académica y administrativa

Además de todas las mejoras pedagógicas descritas en el punto anterior, la implantación de una plataforma educativa integral debe suponer para el centro escolar una clara optimización de múltiples procesos asociados a su funcionamiento.

Las mejoras deben orientarse al interior del propio centro: una gestión más eficiente de toda la carga de trabajo administrativo y de los recursos didácticos; mejoras en la comunicación interna…, y hacia fuera; una mayor implicación de los padres en la vida del centro y en los procesos de aprendizaje; la simplificación de tareas administrativas rutinarias de las familias, como autorizaciones o solicitudes de información...; la estandarización del lenguaje y de los flujos de información, etc. Para que puedan producirse estas últimas mejoras descritas, se hace necesario establecer estándares, sobre todo, de intercambio de datos.

2.5.3 Alfabetización tecnológica de la sociedad motivada por la extensión del uso

Debido al gran número de ciudadanos que son potenciales usuarios de las plataformas educativas, otra gran aportación que pueden realizar, si se generaliza su extensión, es contribuir a la alfabetización digital de la sociedad.

Las posibilidades de las TIC ponen de manifiesto la indudable relación entre innovación y alfabetización tecnológica de la población. Su expansión a todos los ámbitos y estratos de la sociedad se ha producido a gran velocidad y es un proceso que continúa, ya que van apareciendo sin cesar nuevos elementos tecnológicos.

La progresiva disminución de los costes de la mayoría de los productos tecnológicos, fruto del incremento de los volúmenes de producción y de la optimización de los procesos fabriles, se deja sentir en los precios y permite disponer de más prestaciones por el mismo dinero, facilitando la introducción de estas potentes tecnologías en todas las actividades humanas y en todos los ámbitos socioeconómicos[26].

En esta línea de crecimiento, el desarrollo y la rápida difusión de las plataformas educativas parecen contribuir al proceso de enriquecimiento y formación de la sociedad sobre el uso de las nuevas tecnologías. Resulta indudable que los avances científicos y tecnológicos se convierten en verdaderos avances sociales cuando se han popularizado.

[26] Marqués, P. (2005): *Las TIC y sus aportaciones a la sociedad*. UAB

3 POR QUÉ DEBE SER SECURIZADA UNA PLATAFORMA EDUCATIVA

Las plataformas educativas, como cualquier otra aplicación de *software*, debe cumplir unos mínimos estándares de seguridad que garanticen su correcto funcionamiento, de forma que esté disponible cuando se necesite, existan garantías de que los datos se procesarán adecuadamente y que solo accederán a ella las personas autorizadas.

La principal particularidad de una plataforma educativa estriba en el uso masivo que los menores hacen de ella. En cualquier otra aplicación, hay un colectivo de usuarios que se segmentará en función de sus necesidades y atribuciones. Sin embargo, en este caso, una parte muy significativa de este colectivo son menores de edad, por lo que hay que ser muy cuidadoso con la información a la que tienen acceso y la que se recoge de ellos, tanto para cumplir escrupulosamente la ley como para reducir los riesgos y evitar posibles incidentes.

3.1 Expectativas de los usuarios

Como se ha visto, los potenciales usuarios de estas plataformas son todos los actores de la comunidad educativa: administradores de centro, alumnos, profesores, padres, Administración pública, etc. Además de estos usuarios finales, tanto los desarrolladores como el personal que ofrece soporte a estas herramientas están muy interesados en que tengan un adecuado nivel de seguridad.

En general, todos estos usuarios tienen una visión muy concreta de qué esperan de las plataformas en cuanto a su seguridad. A grandes rasgos y con distintos matices, todos coinciden en que:

- La información y los datos personales no deben trascender a usuarios no autorizados, o simplemente a quien no afecte esa información. Por ejemplo, que las calificaciones de un alumno no sean visibles para los padres de otro. Independientemente de la consideración que por ley le corresponda, la información manejada en el ámbito educativo es muy sensible para sus usuarios, por lo que preservar la confidencialidad es fundamental.

- El control de accesos debe ser seguro. No se debe poder acceder a información indebida, solo a aquella relacionada con los trabajos y actividades que se llevan a cabo habitualmente, para evitar que alguien utilice fraudulentamente la información que almacenamos.

- Las plataformas deben estar disponibles siempre que se necesiten, por los múltiples trastornos que ocasionan si no es así: clases canceladas, trabajos no

entregados, tareas administrativas retrasadas, etc. Dado que se utilizan para el trabajo cotidiano de muchas personas, es básico que las aplicaciones no tengan fallos de disponibilidad. Si un profesor que ha preparado su clase no puede acceder a ella en el momento de impartirla, o en el instante de preparar un trabajo no se puede acceder a las herramientas, puede disminuir sensiblemente el grado de utilización de las plataformas.

- Las plataformas deben ser fiables y de fácil utilización, de forma que cualquiera de los usuarios, por bajo que sea su nivel de conocimientos de informática, pueda hacer un uso eficaz y eficiente de los recursos disponibles. Además, debido a que los usuarios dan mucha credibilidad a lo que aparece en los sistemas de información de su entorno educativo, es importante que la información que almacenan sea correcta, completa y fiable.

Sin embargo, cuando entramos en un nivel de detalle superior, observamos que cada grupo de usuarios tiene usos e intereses distintos, lo cual provoca también expectativas diferentes.

3.1.1 Alumnos

El uso de las plataformas por parte de los alumnos está íntimamente ligado a la utilización que sus profesores hacen de las mismas en el aula, y a los recursos tecnológicos y didácticos que posea su centro escolar. Normalmente, se limitan a ser receptores de los materiales que les proponen sus profesores, por lo que su papel está muy limitado. Sin embargo, son un sector de la población que utiliza el ordenador en casa en un alto porcentaje (el 92,4% de los hogares cuentan con ordenador[27], desde el que se conectan a Internet para diversos usos, en muchos casos a diario[28]), y están muy familiarizados con Internet y las herramientas de comunicación, por lo que esperan que las plataformas se puedan usar de la misma manera.

Sus principales expectativas de seguridad son:

- Confidencialidad en las comunicaciones.
- Información correcta y fiable.
- Aplicaciones disponibles.
- Que los accesos sean seguros y fáciles.

[27] INTECO: *Estudio sobre la seguridad de la información y e-confianza de los hogares españoles. Primera oleada (diciembre de 2006-enero de 2007)*. En línea. Disponible en http://www.observatorio.inteco.es

[28] European Commission: Directorate-General Information Society and Media: Safer Internet For Children Qualitative Study In 29 European Countries - National Analysis: Spain. Abril de 2007.

3.1.2 Profesores

Los profesores son los principales motores del uso de las plataformas. Esperan que les proporcionen herramientas que faciliten la preparación de las clases y la transmisión de conocimientos a los alumnos. Con ellas, preparan contenidos y diseñan nuevos modos de impartir la docencia, además de resolver de manera fácil y eficaz las gestiones académicas. Para cumplir estas expectativas, las herramientas deben ser fáciles de utilizar y no dar problemas de disponibilidad. En la medida en que los profesores van percibiendo los distintos usos que les pueden dar a estos recursos, aumenta su utilización[29].

Sus principales expectativas de seguridad son:

- La confidencialidad de los datos y la información.
- La disponibilidad de las aplicaciones.
- La fiabilidad de la información.
- La confidencialidad de las comunicaciones.
- El control de accesos seguro.

3.1.3 Padres

Los padres, en general, tienen un nivel más bajo en el conocimiento de las TIC y, por ello, no plantean demasiadas expectativas iniciales sobre las plataformas. Sin embargo, cuando un centro les ofrece servicios a través de medios digitales, mejora la percepción de la calidad del propio centro y aumenta la demanda de nuevas prestaciones.

Dan por supuesto que las plataformas deben ser “seguras”, entendiendo por ello que no pueda producirse una situación en donde sus hijos tengan acceso a contenidos inapropiados para su edad o alguien no autorizado pueda acceder a sus datos personales o familiares.

Sus principales expectativas de seguridad son:

- La confidencialidad de los datos familiares.
- El cumplimiento de las leyes aplicables.
- El control de accesos seguro.

[29] Centros de Uso Avanzado de las Tecnologías Educativas. IES Doña Jimena: *Informe de evaluación III: curso 2006-2007*.

- La disponibilidad de las aplicaciones.

3.1.4 Dirección de centros escolares

Las direcciones de los centros ven en las plataformas una herramienta de primer orden para administrar las escuelas e institutos (altas, bajas, expedientes académicos, etc.) Sus principales preocupaciones son la disponibilidad, es decir, que la herramienta funcione correctamente en los momentos con mayor carga de trabajo, y cumplir con la Ley Orgánica de Protección de Datos de Carácter Personal[30] (LOPD), ya que cada vez se producen más incidentes y reclamaciones por infracciones a esta ley.

De forma simultánea, el desarrollo de las herramientas de comunicación de las plataformas ha provocado que se generalice su utilización entre los miembros de la comunidad educativa, lo que hace que se planteen cuestiones como la confidencialidad de las comunicaciones (que las notas de los alumnos o las faltas de asistencia vayan exclusivamente a los destinatarios autorizados).

Sus principales expectativas de seguridad son:

- El cumplimiento de las leyes aplicables.
- La confidencialidad de las comunicaciones.
- La confidencialidad de los datos y la información.
- El bajo nivel de incidentes de seguridad.
- La disponibilidad de los equipos.
- La disponibilidad de las aplicaciones.
- El control de accesos seguro.

3.1.5 Instituciones públicas con competencias en educación

La Administración pública tiene un gran interés en que la utilización de las plataformas educativas se vaya extendiendo y popularizando, y cuenta con diversas herramientas y cauces para fomentarlas.

Desde el Ministerio de Educación y Ciencia, se ha impulsado la utilización de las tecnologías de la información y la comunicación en la educación, en particular, con la creación del Centro Nacional de Información y Comunicación Educativa, que busca entre

[30] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). Aparece desarrollado en el Epígrafe 3.3.1 del presente estudio.

sus objetivos apoyar la producción de contenidos curriculares y no curriculares hipermedia, participar en programas y proyectos educativos de la Unión Europea y coordinar las iniciativas de nuevas tecnologías de las comunidades autónomas.

Las plataformas educativas son una potente herramienta que las consejerías pueden usar para acceder de forma rápida a la información relativa a la comunidad educativa, centralizándola y permitiendo una mejor gestión. Por otro lado, las plataformas pueden ser eficaces correas de transmisión de nuevas políticas educativas asociadas con la innovación: nuevas metodologías, atención a la diversidad, desarrollo de capacidades, etc.

El esfuerzo que han hecho muchas comunidades autónomas a través de sus consejerías de educación expresa claramente la voluntad de la Administración por promocionar el uso de las TIC en la escuela. Se espera que las plataformas ayuden en esta tarea; de hecho, es la herramienta fundamental para ello, puesto que se están realizando importantes esfuerzos e inversiones en este sentido.

Las principales expectativas de seguridad de este grupo son:

- El cumplimiento de las leyes aplicables.
- La confidencialidad de las comunicaciones.
- La confidencialidad de los datos y la información.
- El control de accesos seguro.
- El bajo nivel de incidentes de seguridad.
- La disponibilidad de los equipos.
- La disponibilidad de las aplicaciones.

3.1.6 Editoriales

Las editoriales han percibido que las TIC pueden ser una productiva línea de negocio y han empezado a trabajar en ello desde su experiencia como proveedores de material pedagógico con una dilatada trayectoria.

El énfasis, debido a que es la base de su conocimiento, se ha puesto en los contenidos de las plataformas, ya que, en realidad, estas se conciben como complemento del material didáctico en soporte de papel. Los otros aspectos de gestión académica y administrativa y comunicación se están incorporando progresivamente.

Como fabricantes de productos, son más conscientes que otros grupos de usuarios de lo que pueden y no pueden (o no deben) hacer las plataformas, y, a menudo, sus productos superan las expectativas de los usuarios y van creando necesidades. Sus propias expectativas están encaminadas principalmente a difundir los beneficios de las plataformas y expandir su utilización, de manera que su posición en el mercado como proveedores de material pedagógico se afiance o mejore.

Sus principales expectativas de seguridad son:

- La seguridad perimetral de las aplicaciones.
- La seguridad lógica de las aplicaciones.
- La seguridad de las comunicaciones.
- El cumplimiento de la legislación aplicable.
- La integridad de la información.
- La disponibilidad de los equipos.
- La disponibilidad de las aplicaciones.

3.1.7 Consultores de desarrollo

Tienen un perfil muy similar al de las editoriales, pero sin las ventajas ni los inconvenientes de estas como proveedores de material didáctico tradicional de los centros educativos. Sus expectativas sobre la generalización del uso de las plataformas coinciden en muchos puntos con las de las editoriales.

Sus principales expectativas de seguridad son:

- La seguridad perimetral de las aplicaciones.
- La seguridad lógica de las aplicaciones.
- La seguridad de las comunicaciones.
- El cumplimiento de la legislación aplicable.
- La integridad de la información.
- La disponibilidad de los equipos.
- La disponibilidad de las aplicaciones.

3.2 Conceptos de seguridad: confidencialidad, integridad y disponibilidad

Cuando se piensa en la seguridad de la información, lo más habitual es que lo primero que se considere sea mantener a salvo de indiscreciones nuestra información. Sin embargo, cuando los usuarios están en contacto diario con las TIC y, en este caso, con las plataformas educativas, se dan cuenta de que hay otros puntos que tienen también una importancia de primer orden. Este es el caso, por ejemplo, de la información en sí misma, que debe ser mostrada de forma correcta y veraz; lo mismo sucede con el buen funcionamiento de los sistemas de información, que debe estar garantizado frente a problemas técnicos o de suministro. También estos son aspectos de seguridad que hay que tener en cuenta.

Según las normas UNE/ISO-IEC 27001[31], la seguridad de la información se define como la preservación de la confidencialidad, integridad y disponibilidad de la misma, pudiendo estar involucradas, además, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la fiabilidad.

Se entiende por confidencialidad la propiedad de la información por la que esta no se muestra disponible o revelada para individuos, entidades o procesos no autorizados. La integridad es la propiedad de salvaguardar la exactitud y la completitud de los activos de información. La disponibilidad es la propiedad de ser accesible y utilizable por la demanda de una entidad autorizada.

3.2.1 Controles de seguridad

La confidencialidad es el primer concepto que surge cuando se habla de seguridad de la información, incluso a veces se utiliza como término intercambiable, que, evidentemente, no lo es, pero ofrece una idea de la importancia que los usuarios le dan a este aspecto. El que la legislación reconozca la confidencialidad de cierta información como un derecho fundamental, solo añade énfasis a la importancia que se le otorga a este aspecto de la seguridad.

Una información inexacta o incompleta no resulta de mucha utilidad, e incluso puede suponer un problema serio si se utiliza inadvertidamente como si fuera correcta en algún proceso. Por ello, es fundamental utilizar los medios necesarios para que no se produzcan incidentes que comprometan este aspecto de la seguridad.

La disponibilidad es el aspecto más técnico y en el que no siempre se piensa como un tema de seguridad. Esto tiene la ventaja de que en muchos casos existen medidas encaminadas a asegurar la disponibilidad como un procedimiento rutinario, y por ello es un aspecto suficientemente cubierto.

[31] UNE-ISO/IEC 27001 (2007): Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.

Los objetivos de control más habituales, tomados de la lista *Objetivos de control y controles* de las normas UNE/ISO-IEC 27001, que se utilizan para garantizar la seguridad de la información, son los siguientes:

- **Política de seguridad de la información.** Es fundamental contar con unas directrices, por generales que sean, para que todo el mundo sea consciente de la relevancia del tema de seguridad y tenga unos criterios mínimos de actuación. Aspectos que cubre: confidencialidad, integridad y disponibilidad.

- **Organización de la seguridad de la información.** La seguridad es un proceso y, como tal, debe contar con recursos para poder realizarlo y gestionarlo. Los controles de este punto son muy relevantes, puesto que la existencia de un responsable de la seguridad garantizaría un nivel mínimo de la misma. Otro aspecto destacable es que, en sistemas tan complejos como las plataformas, existen muchos implicados que pueden acceder a la información y, por tanto, es crítico que cualquier tercero (subcontratistas, personal de mantenimiento, proveedores, etc.) tenga las mismas obligaciones y responsabilidades que un usuario interno, en especial, en un tema tan sensible como la confidencialidad. Aspectos que cubre: confidencialidad e integridad.

- **Gestión de activos.** Clasificar la información y asignar responsables de su gestión y seguridad evita incidentes dañinos producidos por errores o negligencias, además de facilitar la distribución de medidas de seguridad en función del mayor o menor carácter crítico de la información. Además, que los activos tengan asignado un responsable permite preservar mejor su integridad y, en caso de que surja algún problema, detectarlo y solucionarlo con mayor prontitud. Aspectos que cubre: confidencialidad e integridad.

- **Seguridad.** Es un hecho notorio que todas las medidas tecnológicas aplicadas con el más riguroso criterio pueden resultar inútiles si los usuarios no se preocupan por seguir unas prácticas de seguridad razonables. Por ello, es crucial que todo el personal sea informado y formado en la medida de sus necesidades y responsabilidades, de manera que sean usuarios activos en la protección de la información que manejan en lugar de ser el eslabón débil de la cadena. Otro de los puntos cruciales para garantizar la confidencialidad es la eliminación de todos los modos de acceso a la información que tuviera la persona cuando termina su relación con la organización, devolviendo los activos que poseyera y cancelando los privilegios de acceso con los que contara. Aspectos que cubre: confidencialidad e integridad.

- **Seguridad física y del entorno.** Cualquier medida de seguridad relacionada con el control de accesos es básica para garantizar la confidencialidad y la integridad

de la información, puesto que lo que se pretende evitar es precisamente que alguien no autorizado acceda a ella. Cualquier deterioro que sufran los equipos puede significar una pérdida o filtrado de información, por lo que los sistemas tienen que estar en entornos físicamente seguros para evitar daños que comprometan su seguridad. Aspectos que cubre: confidencialidad, integridad y disponibilidad.

- **Gestión de las comunicaciones y las operaciones.** Que los programas y aplicaciones funcionen como se espera de ellos es indispensable, ya que, en caso contrario, se pueden crear conflictos y errores en el tratamiento de la información que afectarían a la confidencialidad. Esto se aplica igualmente a los servicios que se contratan con terceros, de manera que no surjan discrepancias entre los distintos servicios o que la información que se intercambia no cuente con protección adecuada. Hoy día, las comunicaciones son una herramienta esencial de trabajo, y por ello deben protegerse las redes e infraestructuras en las que se apoyan. Cualquier parte de los sistemas de información implicada en el tratamiento de la información debe ser protegida para garantizar la seguridad de los datos, así como no olvidar que la información no solo reside en los sistemas de información, sino que se maneja en muchos formatos (papel, discos ópticos, dispositivos USB, etc.) vulnerables a sustracciones, copias o pérdidas que ponen en riesgo la confidencialidad. Los aspectos técnicos son muy importantes para garantizar la integridad de la información. En particular, hay que ser muy cuidadosos con la gestión de cambios; la segregación de tareas, de entornos y redes, y la gestión de los servicios que prestan terceros. En este punto, hay varios controles que influyen poderosamente en mantener una disponibilidad adecuada de los sistemas: la planificación y aceptación del sistema, controlar los códigos maliciosos (virus troyanos, gusanos, etc.) y las copias de seguridad. Aspectos que cubre: confidencialidad, integridad y disponibilidad.

- **Control de accesos.** Las normas respecto a los privilegios que cada usuario puede tener deben ser definidas claramente e implementadas con rigor para evitar errores. Si los accesos están correctamente controlados, garantizando que solo los usuarios autorizados acceden a la información pertinente, se impedirá en gran medida que se produzcan incidentes en cuanto a la integridad de la información. A pesar de que el control de usuarios puede impedir errores, es fundamental que los usuarios se comporten adecuadamente de manera que no se produzcan eventos indeseados. Una actitud positiva de un usuario adecuadamente formado puede hacer más por la seguridad que muchas de las medidas técnicas implantadas. Aspectos que cubre: confidencialidad, integridad y disponibilidad.

- **Adquisición, desarrollo y mantenimiento de los sistemas de información.** Debe existir una conciencia clara de cuáles son los requisitos de seguridad de las

plataformas desde el comienzo de su desarrollo por parte de los proveedores de las mismas y por parte de los usuarios que van a adquirirlas, para que puedan evaluar correctamente su adaptación al uso que se le va a dar. Los requisitos de seguridad deberían ser más estrictos cuanto más sensibles son los datos que se van a tratar. Tiene que haber mecanismos que permitan controlar el correcto desarrollo de la aplicación para que no se pueda llegar a las pruebas finales sin haber cumplido con los requisitos establecidos. Aspectos que cubre: confidencialidad, integridad y disponibilidad.

- **Gestión de incidencias de seguridad.** La seguridad perfecta no existe, por lo que siempre ocurrirán incidentes. Cuando esto suceda, debe ser posible tener las herramientas precisas para detectarlos lo antes posible y solucionarlos eficazmente. Para que los errores no repercutan más de lo estrictamente inevitable en la operativa, debe haber una gestión eficaz de las incidencias, poniendo en marcha las medidas necesarias para solucionarlo cuanto antes y minimizar los daños. Aspectos que cubre: confidencialidad, integridad y disponibilidad.

- **Gestión de la continuidad del negocio.** Tener planes de recuperación en caso de desastre es necesario. Los trastornos, si se da el caso, son enormes y pueden ser mitigados eficazmente si se cuenta con un plan claro de actuación que permita recuperar la actividad normal en un plazo razonable, protegiendo así en todo momento la información. Aspecto que cubre: disponibilidad.

- **Conformidad.** No se pueden obviar los requisitos legales, los contractuales y los internos. Para garantizar su cumplimiento, deben establecerse mecanismos sistemáticos que comprueben que se produce la conformidad. Aspecto que cubre: confidencialidad.

3.3 Legislación española relevante

La importancia que reviste la información en nuestra sociedad y la preponderancia que ha tomado la tecnología han sido los impulsores de un cierto nivel de concienciación respecto a la seguridad de la información. Esta realidad novedosa ha provocado que en los últimos años se hayan aprobado múltiples desarrollos legislativos que regulan situaciones que eran una continua fuente de conflictos e irregularidades, y de vulneraciones de derechos fundamentales.

3.3.1 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)

Esta ley se complementa con el reglamento estipulado en el Real Decreto 1720/2007.

El objetivo de esta ley es garantizar y proteger, en lo concerniente al tratamiento de los datos personales (automatizados o no), las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor e intimidad personal y familiar.

Esta ley es un pilar fundamental para garantizar la confidencialidad de los datos personales, que, para el caso que nos ocupa de las plataformas digitales, tiene el agravante añadido de que son datos de menores, y cualquier incidencia con ellos tiene mucha más repercusión en la sociedad y en los medios de comunicación. El cumplimiento estricto de esta ley debe estar contemplado en los requisitos de desarrollo de cualquier plataforma, de manera que facilite la labor a los usuarios y se eviten infracciones fortuitas.

3.3.2 Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones

Junto con su necesario desarrollo reglamentario, esta ley tiene como objeto la regulación de las telecomunicaciones, que comprenden la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas y los recursos asociados, de conformidad con el artículo 149.1.21.ª de la Constitución española.

Muchos entrevistados están de acuerdo en señalar que las comunicaciones van a ser las herramientas más utilizadas a corto y medio plazo en las plataformas. Estas comunicaciones relacionarán entre sí a todos los miembros de la comunidad educativa. Esto implica que hay que tener claro cuáles son las herramientas para proteger las comunicaciones y exigir a sus proveedores un nivel mínimo de servicios que garanticen la seguridad de la plataforma.

3.3.3 Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico

Esta ley regula el régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica.

Las plataformas llevan poco tiempo en el mercado en comparación con otro tipo de aplicaciones, y los servicios que ofrecen son muy heterogéneos, por lo que esta ley puede que no sea de aplicación para todas las plataformas. Pero la evolución lógica será la de ir agregando servicios, y es muy posible que algunos de los contemplados por esta ley acaben siendo proporcionados por la mayoría de las plataformas. Esto supondría que estos requisitos legales deberían ser incorporados.

3.3.4 Ley 59/2003, de 19 de diciembre, de Firma Electrónica

Es una ley que regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

La firma electrónica es uno de los mecanismos de autenticación que los entrevistados han mencionado como posibles sustitutos al tradicional usuario-contraseña. Por otro lado, dado el mencionado aumento de servicios y comunicaciones, utilizar la firma electrónica en la transmisión de información sería un método efectivo de garantizar su seguridad.

3.3.5 Real Decreto Legislativo 1/1996, de 12 de abril, de Ley de Propiedad Intelectual

Esta ley estipula que la propiedad intelectual de una obra literaria, artística o científica corresponde al autor por el solo hecho de su creación.

Para el caso de las plataformas educativas, la propiedad intelectual es un tema que muchos de los entrevistados identifican como problemático, pero que, al no haber tenido hasta el día de hoy consecuencias graves, permanece latente y, en muchos casos, ignorado. La facilidad para localizar y copiar información en formatos digitales hace que en ocasiones y por desconocimiento de que la información utilizada está sujeta a los derechos de propiedad intelectual se pueda vulnerar la normativa.

Una posible solución al problema vendría de la utilización de licencias Creative Commons[32] en los contenidos utilizados por las plataformas educativas.

3.3.6 Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor

Esta ley ofrece un amplio marco jurídico de protección al menor que vincula a todos los poderes públicos, a las instituciones específicamente relacionadas con los menores, a los padres y familiares, y a los ciudadanos en general.

La Ley del Menor es una fuente importante de requisitos para las plataformas digitales. Deben estar diseñadas, desarrolladas, implantadas y gestionadas de manera que se garanticen los derechos reflejados en esta ley. Por otro lado, es una oportunidad para los desarrolladores, la Administración y los gestores de los centros para impulsar los nuevos usos de las TIC en la enseñanza, abriendo nuevos modos de docencia que posibiliten que el menor realmente ejerza sus derechos en un entorno seguro.

3.4 Normativa y buenas prácticas aplicables

Así como muchos de los entrevistados estaban al tanto de, al menos, parte de la legislación vigente que puede ser aplicable a las plataformas digitales, el conocimiento acerca de las normas internacionales y las buenas prácticas ha resultado ser muy

[32] Creative Commons es una organización sin ánimo de lucro que ha desarrollado una serie de documentos legales estándar –licencias de uso– bajo los cuales distribuir contenidos digitales. De este modo, el propietario de los contenidos puede establecer si permite que terceros utilicen una parte o el conjunto de sus contenidos para realizar trabajos derivados con fines comerciales o no. Las licencias Creative Commons permiten reservar algunos derechos y conceder otros. Para más información, consultar http://creativecommons.org/

escaso, estando circunscrito a aquellos profesionales que, de alguna manera, se han encontrado expuestos a la problemática de la seguridad.

Cualquiera de las normas y buenas prácticas que se detallan a continuación puede ser utilizada como referencia para desarrollar políticas y medidas de seguridad para las plataformas educativas, ya que están dirigidas, en general, a los sistemas de información.

Una plataforma educativa es un sistema de información bastante complejo debido a sus peculiares características, con funcionalidades muy variadas y un importante rango de usuarios, pero que comparte con cualquier otro sistema los problemas en cuanto a la definición de requisitos de seguridad y el control interno.

Estas normas son, por tanto, de utilización específica para decidir sobre las medidas de seguridad que hay que implantar, cómo hacerlo y cómo comprobar que funcionan adecuadamente, midiendo el rendimiento de los controles.

3.4.1 La serie de estándares ISO 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización[33] (ISO) y la Comisión Electrotécnica Internacional[34] (IEC). La serie contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener los Sistemas de Gestión de la Seguridad de la Información (SGSI). Los rangos de numeración reservados por la ISO van de 27000 a 27019 y de 27030 a 27044. Las principales normas de esta serie son:

- **ISO 27001.** Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. En su anexo A enumera, en forma de resumen, los objetivos de control y controles que desarrolla la ISO 27002:2005 para que sean seleccionados por las organizaciones en el desarrollo de sus Sistemas de Gestión de Seguridad de la Información.

- **ISO 27002.** Desde el 1 de julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

3.4.2 Cobit

Cobit (Control Objectives for Information and related Technology - Objetivos de Control para Tecnología de la Información y relacionada) es un marco para el gobierno de las TIC

[33] Disponible en www.iso.org

[34] Disponible en www.iec.ch

desarrollado por la Information Systems Audit and Control Association (ISACA)[35] y el IT Governance Institute[36] (ITGI). Además del marco, se proponen herramientas de apoyo que permiten a los directivos establecer relaciones entre los requisitos de control, las cuestiones técnicas y los riesgos del negocio.

La primera versión de los Cobit fue editada en abril de 1996, con el desarrollo de objetivos de control derivados del análisis y estudio de estándares y directrices internacionales, así como de buenas prácticas. Después se desarrollaron directrices para realizar auditorías que evaluaran si estos objetivos de control se habían implantado adecuadamente.

El contenido principal de los Cobit (objetivos de control, directrices de gestión y modelos de madurez) se divide en 34 procesos de TIC, y cada uno de ellos se cubre en cuatro secciones que contemplan cómo hay que controlar, gestionar y medir el proceso.

La última versión Cobit 4.0 pone el énfasis en el cumplimiento reglamentario y en la ayuda a las organizaciones a incrementar el valor obtenido de las TIC; asimismo, permite el alineamiento del negocio y simplifica la implementación del marco.

3.4.3 National Institute of Standards and Technology (NIST)

El National Institute of Standards and Technology[37], dentro del Technology Administration del Departamento de Comercio Estadounidense, fue fundado en el año 1901 con el fin de promover la innovación y la competitividad industrial en los Estados Unidos mediante avances en mediciones, estándares y tecnología, con el fin de mejorar la seguridad económica y la calidad de vida. Para llevar a cabo su misión, disponen de cuatro programas.

- NIST Laboratories, que llevan a cabo la investigación para mejorar la infraestructura en tecnología del país, y apoyar la mejora de los productos y servicios de la industria.

- Baldrige National Quality Program, que promociona la excelencia en los fabricantes, las empresas de servicios, las instituciones educativas y los proveedores de servicios sanitarios.

- Hollings Manufacturing Extension Partnership, una red nacional de centros que ofrecen asistencia técnica y empresarial a pequeños fabricantes.

[35] Disponible en www.isaca.org

[36] Disponible en www.itgi.org

[37] Disponible en www.nist.gov

- Technology Innovation Program, para proporcionar distinciones a la industria, las universidades o los consorcios en investigación en tecnologías potencialmente revolucionarias dirigidas a necesidades críticas del país y la sociedad.

Dentro de los resultados de sus muchas actividades, ha emitido varios documentos con buenas prácticas de seguridad, en particular, el *NIST Handbook An Introduction to Computer Security*[38].

Este manual, redactado en el año 2001, está dirigido a responsables de seguridad de los sistemas de información y a todos aquellos técnicos que necesiten asistencia para comprender los conceptos básicos y las técnicas de seguridad.

El NIST también tiene otras publicaciones de amplia utilización en el entorno de la seguridad informática, tales como la *Contingency Planning Guide for Information Technology Systems*[39] o la *Guide for Developing Performance Metrics for Information Security*[40].

3.4.4 Bundesamt für Sicherheit in der Informationstechnik (BSI, German Information Security Agency)

El Bundesamt für Sicherheit in der Informationstechnik (BSI) tienen como tarea fundamental ser el proveedor principal de seguridad de Tecnologías de la Información (TI) para el Gobierno alemán.

Sus productos y servicios están dirigidos a usuarios y fabricantes de productos de TI, principalmente la Administración pública en los ámbitos federal, regional y local, además de las empresas y los usuarios privados.

Como Agencia de Seguridad Nacional, su objetivo es promocionar la seguridad de las TI, de manera que todo el mundo pueda sacar provecho de las oportunidades de la sociedad de la información.

El BSI ha editado un *The IT Baseline Protection Manual*[41] que contiene medidas de seguridad estándar, consejos de implementación y ayudas para numerosas configuraciones de TIC. La información de este manual tiene como objetivo proporcionar una solución rápida a los problemas de seguridad, apoyar los esfuerzos encaminados a

[38] National Institute of Standards and Technology (2001): NIST Handbook An Introduction to Computer Security. Special Publication 800-12.

[39] National Institute of Standards and Technology (2002): *Contingency Planning Guide for Information Technology Systems, SP 800-34 NIST*. En línea. Disponible en http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

[40] National Institute of Standards and Technology (2006): *Guide for Developing Performance Metrics for Information Security, SP 800-80 NIST's Computer Security Division*, 4 de mayo. En línea. Disponible en http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-80

[41] Federal Office for Information Security (BSI) (2004): *The IT Baseline Protection Manual*. En línea. Disponible en http://www.bsi.bund.de/english/gshb/manual/download/pdfversion.zip

mejorar los niveles de seguridad de los sistemas de información y simplificar la creación de políticas de seguridad de las TIC.

3.5 Metodologías de desarrollo y auditoría de seguridad

La opinión generalizada entre los entrevistados es que una plataforma será tanto más segura cuanto mejor haya sido diseñada y desarrollada, por lo que es importante utilizar metodologías de trabajo y desarrollo que aseguren la ausencia de vulnerabilidades en el código que después puedan ser explotadas por ataques maliciosos o simplemente generen errores. En este sentido, cabe destacar que, aunque existen opiniones y se han dado argumentos a favor tanto del *software* libre como del *software* propietario, la implementación de una u otra solución está más relacionada con razones asociadas a criterios económicos o de facilidad de desarrollo que a argumentos de seguridad. Los profesionales consideran que cualquiera de las opciones es segura si se incluyen los requisitos de seguridad desde el primer momento del desarrollo de la aplicación.

Las principales metodologías reseñadas han sido:

- Estándares para E-learning Management Systems como los desarrollados por Instructional Management Systems (IMS)[42], una asociación sin ánimo de lucro creada en 1997 que lidera el crecimiento y el desarrollo de la industria tecnológica en el campo de la educación y el aprendizaje, mediante la creación de estándares y buenas prácticas o SCORM, una iniciativa del Gobierno de los Estados Unidos desarrollada por Advanced Distributed Learning (ADL)[43], cuyo objetivo es producir cursos con contenidos reutilizables. El Institute of Electrical and Electronics (IEEE) [44] tiene un proyecto estándar, *Learning Objects and Metadata*, entre cuyos objetivos están el facilitar a profesores y alumnos la búsqueda, evaluación, adquisición y utilización de plataformas educativas, y apoyar la seguridad y autenticación necesarias para la distribución y uso de los elementos de aprendizaje.

- *OWASP. Buenas prácticas en programación web segura.* OWASP significa Open Web Application Security Project (Proyecto Abierto de Seguridad de Aplicaciones Web), y es una comunidad abierta dedicada a encontrar y combatir las causas de la inseguridad en el *software* de manera imparcial y práctica.

- *Open Source Security Testing Methodology Manual (OSSTMM), Manual de la Metodología Abierta de Comprobación de la Seguridad,* es uno de los estándares

[42] Disponible en www.imsglobal.org

[43] Disponible en www.adlnet.gov

[44] Disponible en www.ieee.org

profesionales más completos y comúnmente utilizados en auditorías de seguridad para revisar la seguridad de los sistemas desde Internet. Incluye un marco de trabajo que describe las fases que habría que realizar para la ejecución de la auditoría.

4 ANÁLISIS DE RIESGOS

Un análisis de riesgos **consiste en evaluar un conjunto de amenazas en función de su probabilidad de ocurrencia y el impacto que ocasionarían**. En esta sección se pretende exponer las amenazas que perciben los distintos actores involucrados en el desarrollo y utilización de las plataformas educativas, estimar la probabilidad de la ocurrencia de dichas amenazas y considerar los daños que causarían, teniendo en cuenta tanto las diversas opiniones recogidas como las referencias que se encuentran en la literatura.

Para estudiar en detalle la problemática asociada a las plataformas, en primer lugar se han extraído de la información obtenida durante el estudio realizado aquellos puntos en los que se están realizando las tareas de seguridad de una manera acorde con las buenas prácticas establecidas por las normas de la familia ISO 27000.

En segundo lugar, se han descrito los puntos débiles que se han podido identificar. Un punto débil en este contexto es cualquier situación que a) no cumpla con las buenas prácticas establecidas por las normas de la familia ISO 27000, y b), que, de una u otra forma, pueda permitir que ocurra una o más de las amenazas contempladas.

Por último, se ha desarrollado un mapa de riesgos con dos grupos diferenciados. Por un lado, las amenazas debidas a desastres naturales o industriales, y, por otro lado, aquellas que tienen un origen humano. Se han escogido estas amenazas de las propuestas por la metodología Magerit[45], valorando su aplicabilidad en las plataformas educativas. Tras esta selección se han valorado los parámetros de probabilidad de ocurrencia e impacto de caso de la misma, justificando estas valoraciones a la luz de la información recogida.

4.1 Puntos fuertes encontrados

La conclusión más evidente y en la que hay amplio consenso entre los entrevistados es que las plataformas, por tener un zona pública y otra privada a la que se accede mediante identificación de usuario y contraseña, son relativamente seguras para los usuarios, ya que no hay en ellas los mismos peligros que, por ejemplo, se pueden encontrar en Internet. Esto justifica que no se produzcan incidencias frecuentes ni graves. Si no existiera esta separación, se esperaría un volumen de incidencias mucho más elevado, especialmente teniendo en cuenta el importante número de usuarios de las plataformas.

[45] Magerit (2006): *Metodología de análisis y gestión de riesgos de los sistemas de información*. Ministerio de Administraciones Públicas, versión 2.0. En línea. Disponible en http://www.csi.map.es/csi/pdf/magerit_v2/metodo_v11_final.pdf

4.1.1 Seguridad lógica

- **Seguridad perimetral.** Todas las plataformas analizadas, tanto públicas como privadas, tienen, sin haber entrado en la configuración concreta de las reglas, una seguridad perimetral razonable basada en dispositivos conocidos (cortafuegos, balanceadores, filtros de contenidos web, *antispam* y *phishing*, antivirus[46], etc.).

- **Pruebas de intrusión.** En la mayoría de las plataformas encontradas se han realizado auditorías de tipo *hacking* ético por parte de expertos informáticos, aunque no con la frecuencia recomendada, teniendo en cuenta la sensibilidad de la información. Otro aspecto positivo es que en dichas auditorías no se han detectado vulnerabilidades o fallos de gran importancia, que, en todo caso, han sido debidamente resueltos por los responsables de la plataforma siguiendo las recomendaciones emitidas por los expertos tras la auditoría efectuada.

- **Resistencia a virus.** Al ser entornos cerrados, con pocas o ninguna conexión externa, las plataformas están menos expuestas a este tipo de incidencias. Otro de los argumentos que se han dado para explicar el reducido impacto de los virus en ellas es que la mayoría de las plataformas utilizan Unix/Linux, si no completamente, al menos en parte, sistemas operativos para los que apenas se ha desarrollado código malicioso, aunque no por ello se debe caer en la tentación de afirmar que no existe *malware* específico que afecte a Linux[47].

- **Segregación de tareas.** Las plataformas cuentan con múltiples funcionalidades que utilizan información de distinta sensibilidad. Las aplicaciones que gestionan datos sensibles suelen ser separadas lógica e incluso físicamente de las aplicaciones para la docencia. En algunos casos, las aplicaciones para la gestión tienen más controles de acceso o son más rigurosos.

- **Buen posicionamiento internacional.** Hay consenso entre los agentes entrevistados en que el nivel de seguridad lógica de las plataformas en España es similar al del resto de Europa o incluso mayor. Comparado con países como Francia o Alemania, se piensa que España tiene una situación de ventaja, tanto en despliegue de TIC en los centros educativos como en uso de *software* libre.

---

[46] Un cortafuegos (o *firewall* en inglés) es un elemento de *hardware* o *software* utilizado en una red de ordenadores para controlar las comunicaciones, permitiéndolas o prohibiéndolas.
Los balanceadores son dispositivos que se usan para gestionar las solicitudes de un gran número de usuarios en las redes, redirigiendo el tráfico de manera que se eviten los cuellos de botella.
Los filtros web son aplicaciones que permiten filtrar la información que se descarga a cualquiera de los equipos de su red.
Los antispam, *antiphishing* y antivirus son programas que usan varias técnicas para separar el correo basura del deseado, detectar páginas fraudulentas o código malicioso.

[47] INTECO: *Estudio sobre la seguridad de la información y e-confianza de los hogares españoles. Tercera oleada (mayo-julio de 2007)*. En línea. Disponible en http://www.observatorio.inteco.es

4.1.2 Control de acceso

- **Controles eficaces.** Aunque hay mucha diversidad en el tipo de controles y su grado de eficacia, se han encontrado varios que se utilizan en todas las plataformas.
    - Las plataformas utilizan contraseñas para el registro del usuario.
    - Los ficheros de contraseñas y otros datos muy sensibles suelen ser cifrados.
    - Hay una jerarquía de perfiles (alumnos, profesores, administradores, etc.) con distintos privilegios.
    - La utilización queda registrada (*logs* históricos), aunque los periodos de almacenamiento varían mucho, llegando en algunos casos a no cumplir la normativa aplicable.

- **Separación de entornos.** En varias de las plataformas hay una separación física y/o lógica entre las bases de datos sensibles (datos de los alumnos, calificaciones académicas, incidencias escolares, etc.) y el resto del material docente y/o educativo. Esta separación evita que, por ejemplo, los alumnos puedan acceder a datos que no les pertenecen.

- **Ausencia de anonimato.** Las plataformas suelen ser cerradas y no hay anonimato, por lo que el *ciberbullying*[48] es prácticamente inexistente, ya que la facilidad para identificar al culpable es muy disuasoria.

4.1.3 Compra y desarrollo

- **Incorporación de controles de seguridad en los desarrollos.** Los desarrolladores de las plataformas (profesionales y empresas que se dedican al desarrollo de aplicaciones) suelen ser conocedores de los riesgos de seguridad. Los expertos entrevistados han confirmado que, incluso a la hora de desarrollar los proyectos encomendados por las administraciones públicas, han tenido la precaución de incorporar los temas de seguridad con independencia de que estos viniesen establecidos en los pliegos que en convocatoria pública se procedió a publicar. De esta forma, las soluciones entregadas a los clientes-administraciones públicas cumplían con unos estándares de seguridad aceptables. En muchos casos, esto es así debido al propio conocimiento que de la materia tienen los

[48] Se entiende como *ciberbullying* el acoso entre iguales por medio de las nuevas tecnologías (Internet, telefonía móvil o juegos *on-line*). No se circunscribe sólo al ámbito escolar, como ocurre con el *bullying*, y tampoco hace referencia al acecho ejercido por adultos con fines sexuales. En ocasiones, se usan los términos ciberabuso o ciberacoso, pero estas palabras pueden llevar a equívoco por las connotaciones de índole sexual que se les da en otros contextos.

desarrolladores o a que realizan su trabajo a clientes de diversos perfiles que sí incorporan el tema de la seguridad entre los requisitos.

- **La Ley de Contratos**[49]. Establece los criterios que han de regirse en la contratación del sector público, así como entre otros parámetros, y la necesaria solvencia técnica que los empresarios o profesionales han de tener y acreditar a la hora de desarrollar un contrato. En el ámbito de las plataformas, esta ley obliga a los posibles desarrolladores de contenidos a acreditar dicha solvencia, y a los propios adjudicatarios, el poder exigirles que ejecuten la compra de los productos y/o servicios basados en estándares que garanticen que se ajusta a las medidas de seguridad identificadas en este estudio.

4.1.4 Incidencias

- **Bajo número de incidencias.** Los entrevistados coinciden en señalar que las plataformas no generan un número relevante de incidencias, y mucho menos de seguridad. Consideran que este hecho es consecuencia, por un lado, de que los controles de seguridad implantados están funcionando bien y, por otro lado, de que las plataformas no son un objetivo atractivo para los ataques, ya que no contienen información interesante para un potencial atacante.

4.1.5 Concienciación

- **Concienciación sobre seguridad.** Aunque es notoria la falta de formación en seguridad y se considera que hay poca sensibilidad hacia el problema tema en los centros educativos, sí que se ha detectado preocupación por el tema por parte de los entrevistados, que son conscientes de los problemas y situaciones de conflicto que esta situación puede acarrear si perdura en el tiempo.

4.1.6 Cumplimiento de la legislación

- **Observancia de la LOPD**[50]. La mayoría de los entrevistados considera que esta ley, aunque no trate específicamente el tema de los menores, protege adecuadamente sus derechos de intimidad, por controlar con cierta rigurosidad la información personal mantenida y por no permitir su distribución a terceros sin autorización expresa por parte del afectado, que, en este caso, tendría que darse por el padre o tutor. La ley, además, ha ayudado a concienciar a la población en general, incluido el profesorado, en el respeto hacia la intimidad de cada individuo. Por último, se valora que se hayan emitido directrices que permitan orientar los esfuerzos en seguridad, aunque, por parte de los expertos, se echan en falta más

[49] Ley 30/2007, de 30 de octubre, de Contratos del Sector Público. En línea. Disponible en www.boe.es/boe/dias/2007/10/31/pdfs/A44336-44436.pdf

[50] Óp. cit., 30, y más desarrollado en el epígrafe 3.3.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y en el anexo II.

detalles para la implantación de medidas concretas, es decir, que el reglamento fuera incluso más preciso acerca de los pasos que hay que seguir para implantar las medidas de seguridad.

4.2 Vulnerabilidades y otras debilidades detectadas y su impacto

Se define vulnerabilidad en el contexto de seguridad como **aquella debilidad del sistema que permitiría a un atacante comprometer la seguridad del mismo o de los datos**. Hay otra serie de debilidades, por ejemplo, la falta de protección contra incidencias naturales, que no son vulnerabilidades, pero que también podrían comprometer la seguridad de las plataformas.

Las vulnerabilidades suelen estar relacionadas con la confidencialidad de la información, pero un atacante podría también comprometer la integridad de los datos o afectar la disponibilidad de los sistemas. Otras debilidades suelen afectar más a la disponibilidad, aunque también lo podrían hacer a la integridad de la información e incluso, pero con menos frecuencia, a la confidencialidad.

Es muy difícil actuar sobre todas y cada una de las amenazas que pesan sobre las plataformas, dado que la seguridad nunca puede llegar a ser perfecta debido a la evolución constante de nuevas amenazas y a que, cuanto más restrictiva sea la seguridad, menos operativa resulta la plataforma para sus usuarios. Se hace imprescindible encontrar un equilibrio razonable que ha de ser definido en colaboración entre los técnicos de seguridad de las empresas desarrolladoras y los profesionales conocedores de la dinámica de los centros educativos.

El final de la cuestión, por tanto, es determinar la criticidad relativa de los riesgos (medida en términos de su potencial resultado negativo y su probabilidad de ocurrencia) e invertir en medidas de seguridad en consonancia con dicha medición. La cuestión de si es más importante protegerse principalmente contra las vulnerabilidades o contra otras debilidades es importante y depende, hasta cierto punto, de cuál de los tres conceptos de confidencialidad, integridad o disponibilidad sea el más importante. En un banco, la confidencialidad de la información de los clientes, por ejemplo, es de gran importancia, pero la disponibilidad de los sistemas, probablemente aún más. En el caso de las plataformas educativas, la confidencialidad de la información, teniendo en cuenta los posibles riesgos asociados con accesos indebidos a información sensible de menores, es obviamente un aspecto crítico que debería tenerse en cuenta en el momento de diseñar las medidas de seguridad de las plataformas.

Es cierto que entre las fuentes de información, y especialmente en las diversas opiniones expresadas por parte de los entrevistados, las debilidades relacionadas con la confidencialidad se han destacado más. No obstante, aspectos relacionados con la integridad de la información y con su disponibilidad también han sido comentados.

En los puntos que se desarrollan a continuación se resumen las debilidades encontradas durante la fase del trabajo de campo.

4.2.1 Formación y concienciación

- **Falta de formación de los usuarios.** A excepción de los proveedores de las plataformas, que por su trabajo tienen exposición directa con los temas de seguridad, y en sus procedimientos de trabajo llevan incorporadas las herramientas necesarias para que sus aplicaciones cumplan unos requisitos de seguridad, el resto de los actores con implicación en las plataformas educativas carecen seriamente de formación en seguridad; en muchos casos, no tienen formación alguna. De ahí que existan algunas prácticas de riesgo habituales, como compartir las contraseñas, no actualizar los antivirus, no tener en cuenta la propiedad intelectual a la hora de crear contenidos, etc.

- **Falta de concienciación en temas de seguridad.** Los actores implicados más directamente en el uso cotidiano de las plataformas no tienen conciencia de los riesgos que implica este uso. Este comentario fue casi unánime entre los entrevistados y considerado como uno de los problemas más graves actualmente. Es una situación especialmente preocupante en el caso de los alumnos y profesores. La falta de concienciación implica una utilización de las TIC y las plataformas sin unas mínimas precauciones que probablemente en otros ámbitos sí se tendrían.

  En cuanto a los alumnos, no hay conciencia de los riesgos en los que incurren si comparten contraseñas o las establecen excesivamente sencillas. Los profesores, generalmente, no son conscientes de las posibles vulneraciones de la LOPD o de la Ley de Propiedad Intelectual que pueden cometer al crear contenidos o compartirlos. Los equipos directivos de los centros adolecen también de esta falta de concienciación.

  Los desarrolladores y administradores de las plataformas de las consejerías o empresas privadas sí son conscientes de los riesgos que comportan estas aplicaciones, y tienen establecidas medidas que consideran apropiadas, en particular, en cuanto al control de accesos o políticas de definición de perfiles de usuarios y privilegios.

- **Falta de conocimientos técnicos de seguridad.** Esta vulnerabilidad afecta principalmente a los docentes encargados de la coordinación de las TIC (coordinador TIC) de los centros. Estas personas son las que mantienen las plataformas funcionando en el día a día y carecen, en algunos casos, de la formación adecuada para ello, no estando preparados para afrontar los retos tecnológicos que se suceden constantemente. La falta de conocimientos se

vuelve un asunto crítico cuando hay que hacer compras o actualizaciones y no pueden definir los requisitos de seguridad que deberían pedirles a sus proveedores.

- **Dispersión de la información.** No existe mucha comunicación entre centros de la misma comunidad autónoma, y menos todavía entre comunidades, por lo que cada profesor genera sus contenidos sin tener en cuenta otros que hayan podido ser generados por otro colega en otro centro. Se pierde sinergia y se desperdician recursos generando información redundante.

- **Disparidad de la información.** Como en el caso anterior, la información se genera sin considerar trabajos ya existentes en formatos que hacen difícil en cualquier caso compartir la información. Esto impide realizar colaboraciones y reutilizar materiales ya existentes que pueden ser considerados perfectamente válidos.

- **Falta de control de calidad.** Los materiales son utilizados, en la mayor parte de los casos, por sus propios creadores sin haber sido sometidos a revisiones de ningún tipo. Esto es un impedimento serio para la mejora de la calidad de los contenidos.

4.2.2 Seguridad lógica

- **Conexiones de comunicaciones potencialmente poco seguras.** Cuando detrás de la plataforma no existe un equipo técnico preparado y conocedor de la problemática que presentan las comunicaciones y los mecanismos de conexión, se pueden producir incidencias de ataques de código malicioso o incluso intrusiones en los sistemas que, afortunadamente, no se han detectado hasta ahora. La opinión generalizada es que no se ha producido todavía este tipo de ataques, no porque no sea posible, sino porque los atacantes no encuentran atractiva la información a la que podrían acceder. Esto puede cambiar en cualquier momento, por lo que sería necesario un mayor control en las medidas de seguridad relativas a las comunicaciones.

- **Descarga y/o uso de *software* no autorizado.** No debería ser posible descargarlo para evitar problemas de compatibilidad, de código malicioso, vulneraciones a la normativa existente y aplicable, etc.

- **Gestión inadecuada de la red.** Para que las plataformas funcionen adecuadamente, es muy importante que la red en la que están instaladas funcione de manera óptima, para que no se produzcan problemas de disponibilidad ni de errores en el direccionamiento de los flujos de información. Al carecer de personal altamente cualificado en los centros para encargarse de la red, es muy difícil

conseguir una buena gestión de la misma. El buen funcionamiento suele depender en estos casos de la Administración pública competente.

- **Prácticas heterogéneas en cuanto a las copias de seguridad.** En cada centro se hacen las copias de seguridad según el criterio de los responsables del mismo, y, en general, no parece haber una política de copias de seguridad que permita evitar pérdidas de información en caso de incidencias graves. En las entrevistas, se han citado con frecuencia las graves consecuencias que supondría la pérdida de los historiales académicos de los alumnos.

- **Uso inadecuado del *software* o el *hardware*.** Si no existen, a todos los niveles, políticas de seguridad claramente definidas y conocidas por todos los implicados, es muy fácil que se den casos de malas prácticas. Esto implica, por ejemplo, que los sistemas puedan volverse inestables o fallar la disponibilidad de los mismos.

4.2.3 Control de acceso

- **Mecanismos de identificación y autenticación demasiado simples.** El mecanismo que se utiliza sin excepción en la comunidad educativa es el de usuario y contraseña[51]. A pesar de ser prácticamente un estándar universal, hoy en día existen prácticas más eficaces. Sin controles rigurosos sobre la gestión y la calidad de los identificadores, este sistema da lugar a numerosos incidentes; en concreto, los expertos han citado el olvido de contraseñas, el poner contraseñas obvias o demasiado fáciles, y los errores en las altas y bajas de usuarios.

  El gradual aumento del número de contraseñas que un usuario debe utilizar, los distintos grados de autenticación a los que debe someterse, así como la periodicidad con la que se han de cambiar[52], hacen que cada vez sea más complejo y difícil mantener un control de acceso riguroso con este sistema.

  Numerosos entrevistados expresaron su preocupación en este sentido y opinaron sobre cuáles serían los sistemas de identificación y autenticación a medio y largo plazo que sustituirían a los existentes: dispositivos biométricos, tarjetas inteligentes, el DNI electrónico, etc.

- **Controles inadecuados de acceso físico a las instalaciones.** Los centros cuentan con escasos controles de acceso. Cuando se compran e instalan sistemas de información nuevos, esto no conlleva cambio alguno en los controles

[51] Agencia Española de Protección de Datos (2006): *Plan sectorial de oficio a la enseñanza reglada no universitaria*. Madrid, AEPD.
Ídem (2008): *Documento de trabajo 1/08 sobre la protección de datos personales de los niños (directrices generales y el caso especial de los colegios)*. En línea. Disponible en https://www.agpd.es/upload/Canal_Documentacion/Internacional/wp_29/menores_es.pdf

[52] INTECO *Política de contraseñas y seguridad de la información*. En línea. Disponible en http://www.observatorio.inteco.es

de acceso, es decir, a los equipos se puede acceder con facilidad, con el consiguiente riesgo de robos, daños o mal uso de los mismos.

4.2.4 Compra, desarrollo y mantenimiento

- **Falta de definición de los requisitos de seguridad para los desarrolladores.** La falta de conocimientos técnicos, e incluso la carencia de experiencia en el uso de herramientas informáticas en general y de plataformas educativas en particular, ocasiona que los responsables de adquirir estas aplicaciones no sepan qué pueden y qué deben exigir a los proveedores. Al no ser capaces de especificar los requisitos, tanto las funcionalidades que necesitan como las características de usabilidad y seguridad necesarias hacen que se dependa en exclusiva de la competencia técnica y los conocimientos de seguridad de los proveedores. La falta de seguimiento del desarrollo plantea el riesgo de que el código tenga agujeros de seguridad, que lo haga vulnerable a errores o ataques, o de que no cumpla con las necesidades de la comunidad educativa. En el caso de productos comerciales, puede suceder que no se escoja el mejor producto para las necesidades existentes. Por eso, es necesario que se participe activamente en el desarrollo y compra de las aplicaciones, y se exijan unos mínimos a los proveedores.

- **Gestión de las vulnerabilidades conocidas del *software* obsoleto.** Al no existir pautas establecidas ni personal cualificado encargado de gestionar las TIC en los centros, las plataformas se encuentran muy expuestas a fallos de seguridad debido a la falta de actualización del *software* y a los parches de seguridad necesarios.

  Habitualmente, los proveedores facilitan el *software* necesario para actualizar las plataformas. Pero solo cuando la plataforma está alojada en sus instalaciones y los centros acceden en remoto, es cuando se puede estar razonablemente seguro de que se encuentra correctamente actualizada.

- **Mantenimiento inadecuado de los sistemas.** La falta de personal asignado a esta tarea implica que los sistemas estén expuestos a la saturación de los discos duros, la falta de parches, código malicioso oculto (troyanos), etc. Esto provocará un mal funcionamiento de los sistemas y fallos de disponibilidad. Como en el punto anterior, es fundamental que existan recursos humanos y técnicos suficientes para llevar a cabo un mantenimiento apropiado al tamaño y complejidad de los sistemas existentes, de manera que se eviten fallos.

4.2.5 Incidencias

- **Continuidad del servicio.** Apenas existen planes de continuidad en caso de desastre. Los entrevistados han expresado su falta de preocupación, en general,

por el problema. Los centros educativos confían por completo en que, en caso de desastre, la Administración o las empresas proveedoras sean capaces de darles soporte para continuar.

Sin embargo, en algunas consejerías sí que han contemplado este aspecto de la seguridad y cuentan con planes de continuidad para actuar en caso necesario.

4.2.6 Cumplimiento de la legislación y de las normativas

- **Falta de políticas relativas al uso correcto y seguro de las TIC en general y de las plataformas en particular.** Existen centros con políticas de seguridad, pero no es lo más habitual; depende del criterio y la concienciación del equipo directivo del centro. Las consejerías suelen emitir algunas normas de utilización de los recursos informáticos a los centros dentro de su área de influencia, pero no se hace un seguimiento del grado de penetración de estas normas.

- **Incidentes relacionados con la LOPD (privacidad de datos personales, derecho del honor, etc.)**. Se deben en algunos casos por desconocimiento y en otros por falta de concienciación. Estos incidentes pasan inadvertidos en muchos casos, y solo salen a la luz cuando algún implicado denuncia la situación; por ejemplo, a raíz de las quejas de los padres, se ha generalizado la petición de autorización para colgar las fotos de sus hijos en las páginas web de los colegios.

4.3 Mapa de riesgos

Se utilizarán como referencia las amenazas y las dimensiones o aspectos de seguridad documentados en la metodología Magerit[53]. Se han escogido las amenazas que, o bien han sido mencionadas por los entrevistados en algún momento durante el trabajo de campo, o bien se han estimado más relevantes para las plataformas de entre todas las propuestas por la metodología. Las amenazas se han dividido en dos grandes clases: las producidas por error o fallo humano y las que tienen otro origen. Entre estos últimos se encuentran clasificados aquellos que tienen su origen en desastres naturales e industriales (Tabla 1).

[53] Óp. cit., 45.

Tabla 1. Mapa de riesgos: desastres naturales e industriales

Amenaza	Descripción	Dimensiones
Fuego	Incendios: posibilidad de que el fuego acabe con los recursos del sistema.	Disponibilidad. Trazabilidad de los servicios. Trazabilidad de los datos.
	Observaciones: Este riesgo no ha sido contemplado por ninguno de los entrevistados ni por la literatura, sin embargo, el impacto en caso de ocurrir es muy alto y no debe ser obviado.	
Daños por agua	Inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	Disponibilidad. Trazabilidad de los servicios. Trazabilidad de los datos.
	Observaciones: Como en el caso anterior, hay pocas probabilidades de que ocurra, pero el efecto puede ser muy dañino.	
Desastres industriales	Otros desastres debidos a la actividad humana: explosiones, derrumbes, contaminación, accidentes de tráfico, etc.	Disponibilidad. Trazabilidad de los servicios. Trazabilidad de los datos.
	Observaciones: Pocas probabilidades de ocurrir, pero el efecto puede ser muy dañino.	
Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas.	Disponibilidad. Trazabilidad de los servicios. Trazabilidad de los datos.
	Observaciones: Los fallos son relativamente escasos y habitualmente rápidos y fáciles de solucionar, por lo que el impacto no suele ser relevante, con la excepción de daños en los discos, donde el impacto puede ser más grave por pérdida de información.	
Corte del suministro eléctrico	Cese de la alimentación de potencia.	Disponibilidad. Trazabilidad de los servicios. Trazabilidad de los datos.
	Observaciones: Excepto en el caso de que se prolongara el corte, tendría un impacto menos importante.	
Condiciones inadecuadas de temperatura y/o humedad	Deficiencias en la aclimatación de los locales, por lo que hay excesivo calor, frío o humedad.	Disponibilidad. Trazabilidad de los servicios. Trazabilidad de los datos.
	Observaciones: Los equipos y las aplicaciones importantes se encuentran habitualmente en áreas seguras y en condiciones adecuadas.	
Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente, se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender el tráfico presente.	Disponibilidad.
	Observaciones: La mejora en las telecomunicaciones y las exigencias impuestas a los proveedores hacen que este fallo no sea muy probable, pero, cuando ocurre, el fallo de disponibilidad da mala imagen al proveedor o al gestor de la plataforma, y disuade a los usuarios de utilizarla.	
Interrupción de otros servicios y suministros esenciales	Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante, etc.	Disponibilidad.
	Observaciones: La frecuencia con la que ocurra esta amenaza variará según los recursos disponibles en cada centro, pero el impacto no es serio.	
Degradación de los soportes de almacenamiento de la información	Como consecuencia del paso del tiempo.	Disponibilidad. Trazabilidad de los servicios. Trazabilidad de los datos.
	Observaciones: Dependiendo de la sensibilidad de la información contenida en los soportes, el impacto puede ser más dañino.	

Fuente: INTECO

La otra tipología de clasificación de los riesgos es aquellas que tiene su origen en los fallos humanos de los distintos usuarios que acceden a las plataformas educativas, bien por su uso o por el interés que el contenido o los sistemas que las albergan tengan para ellos (Tabla 2).

Tabla 2. Mapa de riesgos: errores o fallos humanos

Amenaza	Descripción	Dimensiones
Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.	Integridad. Disponibilidad.
	Observaciones: La falta de formación en TIC por parte de los usuarios de las plataformas hace que los errores de este tipo sean frecuentes, aunque no suelen revestir demasiada gravedad.	
Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación.	Disponibilidad. Integridad. Confidencialidad. Autenticidad del servicio. Autenticidad de los datos. Trazabilidad del servicio. Trazabilidad de los datos.
	Observaciones.: En general, los administradores están suficientemente cualificados para ejecutar correctamente su trabajo, pero se ha observado que el número de administradores es reducido, y la complejidad de los requisitos y el número de usuarios hacen probable que ocurra. Debido a los privilegios de este tipo de usuarios, el impacto es notable.	
Errores de monitorización (*log*)	Inadecuado registro de actividades: por su falta, por incompletos, por estar incorrectamente fechados, por estar incorrectamente atribuidos, etc.	Trazabilidad del servicio. Trazabilidad de los datos.
	Observaciones: Se ha constatado que a veces no se guardan los *logs* y que la monitorización es inadecuada en ocasiones, por lo que no se detectan los errores, lo que puede ser serio si ocurre algún incidente que haya que investigar (por ejemplo, intentos de un ataque externo).	
Errores de configuración	Introducción de datos de configuración erróneos. Prácticamente, todos los activos dependen de su configuración, y esta, de la diligencia del administrador.	Disponibilidad. Integridad. Confidencialidad. Autenticidad del servicio. Autenticidad de los datos. Trazabilidad del servicio. Trazabilidad de los datos.
	Observaciones: Aunque la responsabilidad de que los sistemas estén correctamente configurados de manera que no se produzcan eventos indeseados esté bien definida, existe falta de criterios acerca de los parámetros que hay que seguir.	
Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión, errores por omisión, acciones descoordinadas, etc.	Disponibilidad.
	Observaciones: No están generalizados los responsables de seguridad ni los accesos a los canales de comunicación con los servicios de soporte, por lo que las acciones pasan por la buena voluntad o conocimientos del que en ese momento se encuentre realizando la tarea.	

Amenaza	Descripción	Dimensiones
Difusión de *software* dañino	Propagación inocente de virus, espías (*spyware*), gusanos, troyanos, bombas lógicas, etc.	Disponibilidad. Integridad. Confidencialidad. Autenticidad del servicio. Autenticidad de los datos. Trazabilidad del servicio. Trazabilidad de los datos.
	Observaciones: Los usuarios no suelen tener acceso a utilidades del sistema y, al estar estos centralizados, incidencias de este tipo no son frecuentes. No obstante, una vez que se produzca la entrada de una aplicación dañina, su propagación será rápida y con consecuencias potencialmente graves.	
Escapes de información	La información llega accidentalmente a personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	Confidencialidad.
	Observaciones: Este es el punto en el que la gran mayoría de los entrevistados coincide en señalar como uno de los más críticos cuando se trata de plataformas educativas. Los datos de menores son, no solo legalmente sino también socialmente, muy sensibles, por lo que cualquier incidente que ponga en peligro su confidencialidad es muy dañino.	
Alteración de la información	Alteración accidental de la información.	Integridad.
	Observaciones: El entorno que usan los menores se espera que contenga información correcta y adecuada para ellos, por lo que, aunque no se produzca con frecuencia, el impacto de un evento de este tipo puede ser importante. Por otra parte, las plataformas contienen información de calificaciones e historiales académicos donde la integridad es también un factor importante.	
Introducción de información incorrecta	Inserción accidental de información incorrecta.	Integridad.
	Observaciones: Como en el caso anterior, que la información que se encuentra en la plataforma sea veraz es un punto básico que hay que cumplir. Puesto que muchos usuarios pueden introducir información en ellas, la frecuencia de que esta amenaza se materialice es considerable y el impacto puede ser importante.	
Deterioro de la información	Degradación accidental de la información.	Integridad.
	Observaciones: Por falta de mantenimiento u otras causas, la información puede degradarse, cosa que ocasionaría un impacto reseñable.	
Destrucción de información	Pérdida accidental de información.	Disponibilidad.
	Observaciones: Por errores de los usuarios o por un mal procesamiento de la plataforma, se puede destruir información que, dependiendo de cuál sea y en qué momento se descubra el hecho, puede crear un trastorno considerable.	
Divulgación de información	Revelación por indiscreción o falta de rigor.	Confidencialidad.
	Observaciones: Esta es otra manera de traicionar la confidencialidad de los datos que, a pesar de no ser intencionada, puede ocasionar un problema importante. La falta de sensibilidad hacia los temas de seguridad lo hace especialmente relevante en los centros educativos.	
Vulnerabilidades de los programas (*software*)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	Integridad. Disponibilidad. Confidencialidad.
	Observaciones: Los entrevistados con un perfil más técnico han señalado que un buen desarrollo del código que genere una aplicación de calidad, sin defectos, es uno de los principales factores que garantizan la seguridad de una plataforma.	

Amenaza	Descripción	Dimensiones
Indisponibilidad del personal	Ausencia del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, etc.	Disponibilidad
	Observaciones: No es un hecho habitual, pero, al no haber mucho personal a cargo de las plataformas, si falta alguien, puede existir un problema de disponibilidad, quizá solo de alguna función.	
Errores de mantenimiento y actualización de programas (*software*)	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.	Integridad. Disponibilidad.
	Observaciones: A pesar de todas las medidas que se tomen, los programas suelen tener fallos que se van descubriendo al utilizarlos, o bien se producen al modificarlos para mejorar sus funcionalidades o su rendimiento. Las plataformas cuentan con numerosos programas y funcionalidades que deben ser adecuadamente mantenidos para evitar costosos incidentes.	
Errores de mantenimiento y actualización de equipos (*hardware*)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	Disponibilidad.
	Observaciones: Evitar esta amenaza es más sencillo cuando hay una entidad central que controla la plataforma, como en el caso de las consejerías, que si lo tienen que hacer los propios centros, dado que a veces no cuentan con personal especializado.	
Caída del sistema por el agotamiento de los recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	Disponibilidad.
	Observaciones: Las plataformas disponen de una gran cantidad de usuarios y la dinámica de la comunidad educativa tiene fechas críticas en las que convergerán muchos de ellos para realizar las mismas tareas (matrículas, evaluaciones, etc.), por lo que esta amenaza es particularmente crítica.	
Manipulación de la configuración	Prácticamente, todos los activos dependen de su configuración, y esta, de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, direccionamiento, etc.	Integridad. Confidencialidad. Autenticidad del servicio. Autenticidad de los datos. Trazabilidad del servicio. Trazabilidad de los datos. Disponibilidad.
	Observaciones: La figura del administrador y sus funciones son críticas para que la plataforma funcione correctamente. Cuando estas funciones están centralizadas, por ejemplo, en las consejerías, es cuando más garantías se pueden dar a los usuarios tanto en seguridad como en funcionalidad, ya que siempre habrá alguien cualificado velando por ello.	
Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la organización o por personal contratado temporalmente.	Confidencialidad. Autenticidad del servicio. Autenticidad de los datos. Integridad.
	Observaciones: Esta amenaza es un ejemplo recurrente de incidente que se quiere evitar a toda costa en una plataforma educativa. No sucede con gran frecuencia, pero el impacto puede ser muy alto, sobre todo si un alumno es capaz de hacerse con los privilegios de un profesor o un administrador, y pudiera ver exámenes o cambiar calificaciones, por ejemplo.	

Amenaza	Descripción	Dimensiones
Abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito. Cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, se producen problemas.	Confidencialidad. Integridad.
	Observaciones: En principio, los usuarios tienen claros sus privilegios, pero algunos usuarios avanzados pueden causar este tipo de problemas.	
Uso no previsto	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal, como juegos, consultas en internet, bases de datos particulares, programas personales, almacenamiento de datos propios, etc.	Disponibilidad.
	Observaciones: Las plataformas tienen unas funcionalidades claras y definidas; aun así, el gran número de usuarios hace factible que ocurran amenazas de este tipo. Debido a las restricciones existentes, se detectará la irregularidad enseguida, y el impacto, en caso de ocurrir, será bajo.	
Reencamina-miento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red que la lleva a donde o por donde no es debido. Puede tratarse de mensajes entre personas, entre procesos, o entre unos y otros.	Confidencialidad. Integridad. Autenticidad del servicio. Trazabilidad del servicio.
	Observaciones: Un entorno cerrado como el de las plataformas no se presta a fallos, intencionados o no, de este tipo. Sin embargo, si ocurre, el impacto puede ser grande, puesto que se pone en juego la confidencialidad de la información, que es el aspecto de seguridad más crítico en las plataformas.	
Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	Confidencialidad. Integridad. Autenticidad del servicio.
	Observaciones: Si el perfil usurpado es el de un profesor, el daño puede ser grave. Para evitarlo, se podrían utilizar sistemas de autentificación, como huellas dactilares.	
Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.	Confidencialidad.
	Observaciones: No parece que se hayan detectado este tipo de eventos, bien porque no se han buscado, bien porque la información que se puede interceptar no es lo bastante atractiva. En cualquier caso, es una amenaza que hay que tener en cuenta, puesto que afecta a la confidencialidad.	
Intercepción de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que esta en sí misma se vea alterada.	Confidencialidad.
	Observaciones: En un entorno educativo existen múltiples oportunidades para interceptar información, por lo que alguien interesado puede esperar el momento oportuno para hacerse con ella. Como en todas las otras amenazas que afectan a la confidencialidad, hay que tenerla en cuenta.	

Amenaza	Descripción	Dimensiones
Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. De origen: negación de ser el remitente u origen de un mensaje o comunicación. De recepción: negación de haber recibido un mensaje o comunicación. De entrega: negación de haber recibido un mensaje para su entrega a otro.	Trazabilidad del servicio.
	Observaciones: Puesto que las comunicaciones todavía no son la parte fundamental de las plataformas, esta amenaza no supone aún un problema mayor. Pero los entrevistados han señalado que las funcionalidades relacionadas con la comunicación serán las que más crezcan a corto y medio plazo, por lo que esta amenaza será más importante.	
Modificación de la información	Alteración intencional de la información con ánimo de obtener un beneficio o causar un perjuicio.	Integridad.
	Observaciones: Los pocos incidentes detectados han tenido escaso impacto. Muchos entrevistados han señalado que la información contenida en las plataformas no parece ser atractiva para los atacantes. Si esta situación cambiara, se deberá reconsiderar esta amenaza.	
Introducción de falsa información	Inserción interesada de información falsa con ánimo de obtener un beneficio o causar un perjuicio.	Integridad.
	Observaciones: Suele haber una estricta observancia de los privilegios de cada nivel de usuario, por lo que los usuarios autorizados para introducir información son personal perfectamente capacitado y fácilmente identificable, lo que en principio es disuasorio. No obstante, el impacto, especialmente en el caso de la inserción de material no apropiado, podría ser grave.	
Corrupción de la información	Degradación intencional de la información con ánimo de obtener un beneficio o causar un perjuicio.	Integridad.
	Observaciones: Como en el caso anterior, este tipo de amenazas es fácilmente detectable e imputable en un entorno tan controlado, por lo que no es fácil que ocurra.	
Destrucción de la información	Eliminación intencional de información con ánimo de obtener un beneficio o causar un perjuicio.	Disponibilidad.
	Observaciones: Un ataque de este tipo puede ser muy dañino, por lo que habrá que tomar medidas para que no se produzca.	
Divulgación de la información	Revelación de información.	Confidencialidad
	Observaciones Al haber tantos implicados alrededor de las plataformas, este es un incidente que puede ocurrir fácilmente y, si la información es relevante o llega a un lugar que no debiera, el daño puede ser importante.	
Manipulación de programas	Alteración intencionada del funcionamiento de los programas, posiblemente persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	Confidencialidad. Integridad. Autenticidad del servicio. Autenticidad de los datos. Trazabilidad del servicio. Trazabilidad de los datos.
	Observaciones: Este es un tipo de ataque que no se ha detectado todavía. En el caso de que ocurriera, podría generar daños de importancia dependiendo de cuál fuera la información que se llegara a manejar fraudulentamente y cuál fuera el uso que se le diera.	

Amenaza	Descripción	Dimensiones
Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. Esta situación puede ser causada también por ataques externos deliberados.	Disponibilidad.
	Observaciones: Una de las características de las plataformas es el gran número de usuarios que las utilizan, en mucho casos, de manera concurrente, por lo que es importante tener en cuenta esta amenaza, ya que el que la aplicación no esté disponible desmotiva a los usuarios para utilizarla. Por otra parte, las plataformas no suelen ser objetos deliberados de ataques de denegación de servicio.	
Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir, una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el de equipos y el de soportes de información los más habituales.	Disponibilidad. Confidencialidad.
	Observaciones: Esta es una amenaza que hay que tener en cuenta, puesto que no todos los centros cuentan con seguridad adecuada y los equipos informáticos siguen siendo interesantes. En principio, los equipos destinados a los usuarios no deben albergar información; esta debería estar en el CPD donde se aloje la plataforma, por lo que la confidencialidad estaría a salvo, pero los usuarios no dispondrían de medios para utilizar la plataforma durante un tiempo, con todos los inconvenientes que esto puede conllevar.	
Ataque destructivo	Vandalismo, terrorismo, acción militar, etc. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la organización o por personas contratadas de forma temporal.	Disponibilidad.
	Observaciones: Una amenaza de este tipo, con su alto impacto en caso de que ocurra, es lo que hace que sean imprescindibles los planes de contingencia, para que, si llega a suceder, se pueda recuperar la actividad normal en un plazo razonable de tiempo.	
Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	Confidencialidad. Integridad. Autenticidad del servicio. Autenticidad de los datos. Trazabilidad del servicio. Trazabilidad de los datos.
	Observaciones: Cuando esta amenaza se produce, estamos hablando de acoso. La falta de anonimato que se da en las plataformas hace muy difícil que se den casos de este tipo, así como el escaso uso de las herramientas de comunicación, que son los principales medios de realizar este tipo de actos.	
Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades o divulguen información (por ejemplo, códigos de acceso) que interesa a un tercero.	Confidencialidad. Integridad. Autenticidad del servicio. Autenticidad de los datos. Trazabilidad del servicio. Trazabilidad de los datos.
	Observaciones: El alto grado de conocimiento de los usuarios entre sí y sus relaciones de confianza favorecen muchísimo este tipo de amenazas. Hay que formar muy bien a los usuarios para que distingan las prácticas de riesgo.	

Fuente: INTECO

Cada una de las amenazas se ha valorado en función de la probabilidad de que ocurra y del impacto que ocasionara en una escala de tres valores, alto, medio y bajo, con el único fin de ponderar el riesgo y reflejar dónde han puesto el énfasis los entrevistados.

La primera clasificación hace referencia a los desastres provocados por la naturaleza o por fallos industriales ajenos a la voluntad de los individuos. No obstante, y tal y como se puede comprobar en la Tabla 3, aunque su probabilidad es mínima en la mayoría de los casos, esto no se ve reflejado en el impacto que dichas acciones pueden tener en las plataformas educativas. En lo que respecta a la Tabla 4, aparece reflejado el mapa de amenazas relacionadas con los errores humanos. A diferencia de los datos recogidos en la anterior tabla, los fallos humanos tienen una probabilidad mayor de ocurrir, lo que conlleva un impacto más grave.

Tabla 3. Mapa de amenazas de desastres naturales e industriales en función de la probabilidad de que ocurran y del impacto

	Probabilidad			Impacto		
Amenaza	**Alta**	**Media**	**Baja**	**Alta**	**Media**	**Baja**
Fuego			X	X		
Daños de agua			X	X		
Desastres para las industrias			X	X		
Avería de origen físico o lógico			X			X
Corte del suministro eléctrico			X			X
Condiciones inadecuadas de temperatura y/o humedad			X			X
Fallos de servicios de comunicaciones			X		X	
Interrupción de otros servicios y suministros esenciales		X				X
Degradación de los soportes de almacenamiento de la información			X		X	

Fuente: INTECO

Tabla 4. Mapa de amenazas de errores o fallos humanos en función de la probabilidad de que ocurran y del impacto

	Probabilidad			Impacto		
Amenaza	**Alta**	**Media**	**Baja**	**Alta**	**Media**	**Baja**
Errores de los usuarios	X				X	
Errores del administrador		X			X	
Errores de monitorización (*log*)		X			X	
Errores de configuración			X		X	
Deficiencias en la organización	X				X	
Difusión de *software* dañino			X	X		
Escapes de información		X		X		
Alteración de la información		X		X		
Introducción de información incorrecta		X			X	
Degradación de la información		X		X		
Destrucción de la información		X		X		

	Probabilidad			Impacto		
Amenaza	**Alta**	**Media**	**Baja**	**Alta**	**Media**	**Baja**
Divulgación de la información		X		X		
Vulnerabilidades de los programas		X		X		
Errores de mantenimiento y actualización de programas		X			X	
Errores de mantenimiento y actualización de equipos (*hardware*)		X			X	
Caída del sistema por agotamiento de recursos.		X		X		
Indisponibilidad del personal.			X			X
Manipulación de la configuración			X	X		
Suplantación de la identidad		X		X		
Abuso de privilegios de acceso		X			X	
Uso no previsto			X		X	
Reencaminamiento de mensajes			X	X		
Acceso no autorizado	X				X	
Análisis de tráfico		X			X	
Repudio			X		X	
Intercepción de información			X		X	
Modificación de la información			X		X	
Introducción de falsa información			X	X		
Corrupción de la información			X		X	
Destrucción de la información			X	X		
Divulgación de información	X			X		
Manipulación de programas			X		X	
Denegación de servicio		X		X		
Robo			X	X		
Ataque destructivo			X	X		
Extorsión		X		X		
Ingeniería social	X			X		

Fuente: INTECO

4.4 Potenciales amenazas

Como se ha destacado en varios puntos de este informe, la seguridad de las plataformas educativas no está siendo un problema importante en la actualidad. Sin embargo, algunos de los entrevistados han dibujado un futuro diferente en el que la seguridad se verá más comprometida. Esta evolución estará ligada a la generalización del uso de las plataformas y al incremento de las funcionalidades soportadas, especialmente las relacionadas con la comunicación y el manejo de datos más sensibles e interesantes para potenciales atacantes.

La sensación de seguridad que vivimos actualmente no está sustentada por datos concretos, sino por el bajísimo número de incidencias. Es probable que la ausencia de sistemas eficaces de detección y gestión de incidencias nos esté ocultando la existencia de más que las que se producen actualmente. Además, esta sensación de seguridad se

deriva también de la falta de un análisis de riesgos que pudiera poner en evidencia cuáles son los puntos críticos de este tipo de aplicaciones. Ninguno de los actores implicados en el desarrollo y utilización de las plataformas ha realizado un análisis de riesgos de este tipo, por lo que pueden existir problemas latentes que aún no han sido identificados.

Como se ha comentado anteriormente en este estudio, muchos entrevistados han comentado que el bajo número de incidencias puede crecer si la información almacenada en las plataformas se vuelve atractiva por algún motivo. Los usos que se hacen de la tecnología cambian continuamente y la información que se almacena varía. Hace cinco años, nadie contemplaba la posibilidad de que fuese necesario tener que autorizar la publicación de la foto de su hijo, pero en la actualidad se ha convertido en un requisito legal. Como no es posible prever ahora mismo qué tipo de información se irá incorporando a las plataformas a medio y largo plazo, es necesario evaluar los riesgos a los que se expone la información con regularidad. De esta manera, se pueden ir tomando decisiones informadas acerca de las medidas de seguridad que es necesario incorporar a medida que cambian las necesidades.

Otro aspecto que ahora mismo no presenta problemas serios es el de la disponibilidad. Sin embargo, puesto que se espera que el número de usuarios crezca considerablemente a corto y medio plazo, sería necesario realizar un estudio para poder prever la capacidad que deberían tener los sistemas para poder ofrecer un servicio de calidad en momentos puntuales en los que está previsto que se produzcan picos importantes de concurrencia (matriculación, evaluaciones, solicitudes de becas, periodo de escolarización) debido a una mayor utilización de los recursos o a una mejora de las propias plataformas.

Las comunicaciones han sido mencionadas en varias entrevistas como las herramientas que presentan mayores posibilidades de desarrollo a corto plazo. Es previsible que en poco tiempo se dote a los usuarios de potentes medios de comunicación para intercambiar todo tipo de datos e información. Paralelamente a este aumento de funcionalidades, deben incrementarse los mecanismos de control orientados a evitar que la seguridad de la información y los usuarios se vea comprometida. Por un lado, la autenticación de los usuarios debe ser estricta, haciéndose fundamental la identificación inequívoca de todos los usuarios de las plataformas. Por otro lado, deben evitarse intercepciones de estas comunicaciones, desvíos y errores en la entrega de los mensajes, que pueden ser confidenciales, y asegurarse de que los destinatarios son únicamente los intencionados.

5 NECESIDADES DETECTADAS

El análisis realizado a lo largo de las secciones anteriores ha permitido tener una idea aproximada del escenario en el que se desarrollan el diseño, construcción, implantación y utilización de las plataformas educativas en nuestro país.

Este análisis está alineado con los objetivos del estudio, que, al detallar cuáles son los de cada colectivo implicado y compararlos con la realidad que han expuesto los entrevistados y las recomendaciones de normas, leyes y buenas prácticas existentes, permiten detectar las necesidades que se están creando en torno al incipiente uso de las plataformas.

Ha quedado demostrado a lo largo del estudio que es necesario seguir impulsando el desarrollo de la política de seguridad de las plataformas educativas. Esta necesidad viene motivada por diversos factores; así, los desarrolladores no creen que una política de seguridad específica en este entorno sea necesaria, dado que los contenidos de las mismas no son objeto de posibles incidencias. Además, puesto que hasta el momento no se habían dado casos en los que los sistemas que albergan las plataformas hayan sufrido vulnerabilidades, no se había planteado la securización de las mismas. Por parte de los administradores y usuarios, el nivel de uso y el rendimiento que puedan extraer de estas está limitado por la falta de formación de los mismos. La mayoría de los expertos participantes en el estudio coinciden en señalar:

- Que para sacar todo el partido a estas plataformas es necesario atender y garantizar cuatro pilares básicos: conectividad, disponibilidad de recursos tecnológicos, disponibilidad de contenidos didácticos y formación del profesorado.

- Que un incidente serio de seguridad dañaría la credibilidad de estas herramientas, y frenaría el desarrollo del sector y la difusión de su uso.

- Que el cumplimiento estricto de la LOPD y el el nuevo reglamento de desarrollo de la LOPD (RDLOPD) deben estar contemplados en los requisitos de desarrollo de cualquier plataforma, de manera que se facilite la labor a los usuarios y se eviten posibles infracciones.

- Que la confidencialidad de la información, teniendo en cuenta los posibles riesgos asociados de acceso a información (familias y menores), es obviamente un aspecto crítico que debería tenerse en cuenta en el momento de diseñar las medidas de seguridad de las plataformas.

- Que se ha identificado el tema de la propiedad intelectual como un asunto sensible, que sin embargo, hasta el día de hoy no ha tenido consecuencias

graves, permaneciendo latente y, en muchos casos, ignorado. Una posible solución al problema vendría a través de la utilización de licencias abiertas, del tipo Creative Commons, en los contenidos utilizados por las plataformas educativas.

- Que la sensación de seguridad que vivimos actualmente no está sustentada por datos concretos, sino por el bajísimo número de incidencias. Además, esta sensación se deriva también de la falta de un análisis de riesgos que pudiera poner en evidencia cuáles son los puntos críticos de este tipo de aplicaciones.

Tomando en consideración las opiniones de los expertos y la situación real de las plataformas, las necesidades que existen a corto, medio y largo plazo, INTECO las identifica a continuación por los siguientes ámbitos de actuación:

- **Sensibilización, formación e información.** Los usuarios y proveedores de servicios han de conocer la necesidad de establecer criterios de seguridad que cubran los aspectos de privacidad que pudieran ser vulnerados, así como los contenidos educativos incluidos en los mismos[54].

  Para un desarrollo seguro de las plataformas es necesario que se cuente con usuarios formados[55] a todos los niveles[56] (alumnos, personal docente y no docente, administradores de sistemas, editoriales, etc.), para garantizar el uso correcto de las mismas y evitar la aparición de errores y que se puedan realizar tareas de manera incorrecta. Para ello se han de introducir mecanismos de validación sobre los que previamente han sido formados.

  Asimismo, se hace necesaria la divulgación en este aspecto para cubrir los aspectos señalados anteriormente tanto en materia de seguridad de la información como en aquellos otros que tienen que ver con el uso responsable de Internet[57].

---

[54] Para facilitar el desarrollo de estos criterios se han puesto en marcha programas en la Unión Europea, como el Safer Internet Plus, que promulgan el desarrollo de actividades basadas en cuatros líneas de actuación (lucha contra los contenidos ilícitos, tratamiento de los contenidos no deseados y nocivos, fomento de un entorno más seguro y sensibilización). En línea. Disponible en http://ec.europa.eu/information_society/activities/sip/index_en.htm

[55] Junge, Kerstin, y Hadjivassiliou, Kari (2007): *What are the EU and member states doing to address digital literacy? E-learning Papers*, núm. 6. ISSN 1887-1542.

[56] En el ámbito europeo estos esfuerzos se plasman en el desarrollo de iniciativas encaminadas a mejorar las competencias digitales mediante por ejemplo la inclusión en los currículos de competencias más amplias sobre temas de seguridad y navegación segura en Internet (como el programa "Ligar Portugal") o la creación de una red para los profesores para que además de formarse en herramientas de *e-learning*, desarrollen material conjunto que después pueda ser puesto a disposición de toda la comunidad escolar (como el proyecto Opinpolku). En línea. Disponible en http://www.ligarportugal.pt/ y en http://www.opinpolku.com/www/

[57] En el Reino Unido la British Educational Communications and Technology Agency (BECTA), esto es, la agencia del gobierno británico para las tecnologías de la información y comunicación en educación, como parte del esfuerzo para alcanzar este objetivo, ha desarrollado una herramienta estratégica resultado de la colaboración con 38 autoridades

- **Normativa.** Se hace necesario velar por el cumplimiento de la normativa ya existente y asegurar el buen uso de los datos susceptibles de ser utilizados con otros fines de los que fueron creados.

- **Certificación y estandarización.** Las mejoras proporcionadas por las plataformas deben producirse hacia dentro del propio centro, basándose en una gestión más eficiente de la carga de trabajo administrativo y de los recursos didácticos y/o mejoras en la comunicación interna y hacia fuera, a través de una mayor implicación de los padres en la vida del centro y en los procesos de aprendizaje, de la simplificación de tareas administrativas rutinarias de las familias, como autorizaciones, y de la estandarización del lenguaje[58] y de los flujos de información. Para ello, es necesario que se establezcan estándares o que se certifiquen las buenas prácticas existentes, sobre todo de intercambio de datos.

  Paralelamente a este incremento de funcionalidades, es necesario aumentar los mecanismos de control orientados a evitar que la seguridad de la información y los usuarios se vea comprometida.

- **Funcionalidad.** La extensión del uso de las plataformas educativas es una realidad y, asimismo, una oportunidad para los desarrolladores, la Administración Pública y los gestores de los centros de impulsar el uso de las TIC en la enseñanza, abriendo nuevos modos de docencia que posibiliten que los alumnos, menores o no, puedan desarrollarse en un entorno seguro.

  Una generalización del uso de las plataformas y del incremento de las funcionalidades soportadas, especialmente las relacionadas con la comunicación y el manejo de datos más sensibles e interesantes para potenciales atacantes, hace necesario establecer mecanismos que garanticen la continuidad de las mismas[59]. Como no es posible prever ahora mismo qué tipo de información se irá incorporando a las plataformas a medio y largo plazo, es necesario evaluar los riesgos a los que se expone la información con regularidad; de esta manera, se

locales, 5 consorcios regionales de banda ancha, y representantes de Escocia, Gales y la Unión Europea. Se ha desarrollado con la idea de facilitar que se compartan buenas prácticas, y ofrecer apoyo y guía para que las autoridades locales garanticen la seguridad online de los niños y los estudiantes. Incluye numerosas recomendaciones en varias áreas, entre ellas, cómo desarrollar una infraestructura segura, cómo proyectar una estrategia de formación en seguridad, o la monitorización y comunicación de incidentes. Más información disponible en BECTA (2008): *Safeguarding children in a digital world. Developing an LSCB e-safety strategy*.

[58] Un ejemplo del uso de estándares adaptados a la diversidad de plataformas, dispositivos e idiomas que se utilicen es la iniciativa de Intel Skoool basada en la tecnología Skoool™. En línea. Disponible en http://www.skoool.com, http://www.skoool.co.uk y http://www.skoool.es

[59] En el Reino Unido previendo la complejidad de las mismas, BECTA ha elaborado una guía sobre seguridad en el uso de las TIC para centros educativos. Más información disponible en BECTA, ICT (2004): *Essential guides for school governors, Safety and security with ICT*.

pueden ir tomando decisiones acerca de las medidas de seguridad que es necesario incorporar según cambien las necesidades.

Otro aspecto que ahora mismo no presenta problemas serios es el de la disponibilidad, aunque, como se espera que el número de usuarios crecerá considerablemente a corto y medio plazo, habrá que realizar un estudio de la capacidad que tendrán que tener los sistemas para ofrecer el servicio de calidad que se espera, con independencia de que existan momentos puntuales en los que se puedan producir picos importantes de concurrencia (matriculación, evaluaciones, solicitudes de becas, periodo de escolarización, etc.).

- **Seguridad de contenidos.** Es importante evitar las posibles intercepciones en las comunicaciones y entrega de mensajes, ya que estos pueden ser confidenciales. Es por ello por lo que debería asegurarse la autenticación de los destinatarios mediante el uso de sistemas de cifrado de la información o mediante la propia firma digital.

  No obstante, es importante que existan procedimientos de actuación para que se gestionen las plataformas de forma correcta por todos los usuarios, priorizando la gestión de la capacidad, la actualización y el parcheado de los programas. Por otro lado, la existencia de amenazas obliga a dotar de recursos técnicos y humanos adecuados a las tareas de operación y mantenimiento de las plataformas, de manera que su funcionamiento sea óptimo en todo momento y se eviten los riesgos de un mantenimiento defectuoso.

6 RECOMENDACIONES Y PROPUESTAS

A la luz de las necesidades identificadas en el epígrafe anterior, podemos señalar algunas propuestas y recomendaciones que los diferentes actores y usuarios de las plataformas educativas que son objeto de este estudio, esto es, aquellas del ámbito enseñanza primaria y secundaria, y de los servicios que llevan inherentes deberían tener en cuenta en el ámbito de la seguridad de la información. Dichas recomendaciones deben estar presentes a la hora de:

- Establecer los criterios para diseñar las plataformas.
- Desarrollar y controlar los contenidos y utilidades.
- Usar las plataformas.

De esta forma, se pueden mejorar los niveles de seguridad que existen actualmente en el marco de las plataformas educativas.

Las recomendaciones y propuestas de mejora que desde INTECO se proponen son:

6.1 Sensibilización, formación e información

- **Desarrollar programas de sensibilización, formación e información para todos los usuarios de las plataformas educativas sobre temas de seguridad.** Los esfuerzos se han de centrar en la formación en los ámbitos de la difusión, la divulgación y la comunicación, y respecto a los cursos, dada la diversidad de agentes, podría optarse por la teleformación. El trabajo con los padres de los alumnos puede estar liderado desde el propio centro escolar de sus hijos, que, en colaboración con la Administración pública, puede organizar charlas, jornadas o campañas informativas en los colegios; divulgar la documentación mediante guías que tengan en cuenta los aspectos prácticos de la gestión de la seguridad; realizar encuestas que velen por la satisfacción de los usuarios y a su vez sirvan para valorar su nivel de conocimiento, y/o herramientas de seguridad de acceso no solo a las plataformas, sino que le garanticen un uso responsable de Internet.

  En el caso de la formación basada en normativas o incluso en la legislación existente, como, por ejemplo, la familia de los estándares ISO/IEC 27000, buenas prácticas o la LOPD, sería necesario que algún organismo oficial facilitase la labor mediante la elaboración de guías que puedan extraer los aspectos relevantes al entorno escolar y en las plataformas educativas.

- **Formar a los alumnos** de manera transversal dentro del currículo en materia de seguridad para garantizar el buen uso de los recursos de los que disponen y para

que sean transmisores de la información a su entorno más cercano. La apuesta por la utilización de los recursos docentes puede desarrollarse mediante la utilización de las publicaciones de los centros para difundir dicha información.

- **Divulgar desde los medios de comunicación.** Estos pueden convertirse en los grandes aliados en la estrategia de concienciación y sensibilización sobre la seguridad.

6.2 Normativa

- **Enfocar la legislación a los usos que se pueda hacer de la información,** exigiendo responsabilidades tanto a aquellos que acceden de manera ilícita a la misma o hagan un uso fraudulento o poco ético, así como a los que, por incumplimiento grave en su deber de custodia o gestión, comprometan su seguridad. Penalizar estos actos tendría un fuerte efecto disuasorio.

- **Generalizar la utilización de acuerdos de confidencialidad para proteger la información.** Aquellas personas que por su trabajo o situación en la organización vayan a tener acceso a información sensible, aun cuando la LOPD y el nuevo reglamento de desarrollo de la LOPD (RDLOPD) no la contemple como de nivel alto, deberían firmar un acuerdo de confidencialidad que evite o al menos dificulte que se produzcan situaciones de riesgo. Otra medida que se puede tomar en este sentido es la de formalizar la devolución de los activos que se hayan entregado a los usuarios cuando finalice su relación con la organización, así como la cancelación de los derechos de acceso para evitar que se produzcan accesos no autorizados y potencialmente peligrosos en el caso de que la salida de esa persona de la organización no haya sido pactada.

6.3 Certificación y estandarización

- **Generar especificaciones funcionales y técnicas de las plataformas que incluyen los requisitos de seguridad.** De esta forma, las normas servirán de guías tanto a los compradores, que sabrían qué necesitan exigir, como a los desarrolladores, que tendrían claro qué es lo que los clientes buscan y esperan. Se deberían especificar los requisitos mínimos de seguridad para una correcta instalación, un óptimo uso y un adecuado mantenimiento de las plataformas, y, así, gestionarlas con eficiencia a lo largo de todo su ciclo de vida.

  De igual modo, sería útil contar con estándares de calidad y buenas prácticas internacionales para la utilización de las plataformas adaptándose a lo identificado y desarrollado en este estudio; por ejemplo, la serie de estándares ISO 27000.

- **Certificar los criterios previamente establecidos por la Administración pública** o una entidad de reconocido prestigio. Asimismo, los desarrolladores

deberían certificar la calidad de sus metodologías de trabajo y los criterios que utilizan para garantizar la seguridad de los desarrollos. Por último, las administraciones educativas y los centros escolares deberían certificar la gestión de la seguridad de la información.

6.4 Funcionalidad

- **Flexibilizar y operativizar el funcionamiento de las plataformas,** lo que llevaría a una posible autorregulación[60] de las mismas con vistas a la asunción interna de las normas que deben regir su actividad. Esto es aún más necesario en aquellas plataformas que se han creado mediante distintos desarrollos, *software* libre o propietario, lo que hace incompatible su gestión común.

- **Mejorar la seguridad física de las áreas en las que se pueden utilizar las plataformas,** ya que, en muchos casos, el acceso físico es muy sencillo y se presta a posibles situaciones de riesgo. Los equipos que alberguen información sensible o sean susceptibles de utilizarse para acceder a ella deberían estar en entornos protegidos de una manera razonable contra accesos no autorizados. En el caso de que no sea factible, por ejemplo, en áreas comunes de los centros educativos con acceso público, se deben establecer controles lógicos más restrictivos que impidan el acceso a las aplicaciones. Por supuesto, esto no se aplicará a los desarrolladores de plataformas, que, en todo caso, deberían contar con controles de acceso para asegurar que solo el personal autorizado puede entrar en las instalaciones y en los centros de proceso de datos de las consejerías; es por ello por lo que deben ser muy restrictivos en cuanto a sus privilegios de acceso. Además de controlar los accesos, se deben tener en cuenta las medidas anti incendios previstas por la legislación vigente, así como de otras orientadas a evitar daños en caso de desastres naturales, como inundaciones o viento, que pueden causar graves trastornos.

- **Gestionar la capacidad.** Se ha comentado en varios apartados del estudio la inquietud que suscita entre los entrevistados de perfil más técnico la posibilidad de que el aumento de usuarios llegue a provocar fallos en los sistemas debido al colapso de los mismos por falta de capacidad. Esto es especialmente crítico en el caso de picos de trabajo de la comunidad educativa, como los periodos de matriculaciones o emisión de notas. Por ello, sería un avance importante que la gestión de la capacidad se incorporara de manera paulatina a la gestión de los sistemas de información involucrados en la utilización de las plataformas. Hay que hacer un seguimiento detallado de la incorporación de usuarios, de los niveles de

[60] Se define la autorregulación como el proceso voluntario de control y monitorización interna que tiene una organización con capacidad para el análisis real de las situaciones.

tráfico, de los periodos de más uso y, en general, de cualquier parámetro que indique un requisito de capacidad de los sistemas para poder planificar las necesidades con un cierto margen de tiempo. De esta manera, se pueden establecer las acciones necesarias para proveer a los usuarios de la capacidad que van a necesitar, y asegurar que los sistemas se mantendrán ajustados a la realidad del uso que se hace de ellos.

- **Dar más importancia al diseño de las plataformas,** en el sentido de que estén pensadas de manera que sea difícil que los usuarios puedan cometer fallos. Por ejemplo:
    - Que, en la medida que sea posible, no se pueda introducir información errónea o inconsistente.
    - Que haya separaciones lógicas e incluso físicas entre los diversos grupos de usuarios con distintos niveles de privilegios, para que no accedan a información o aplicaciones a las que en principio, y en función de su perfil, no deberían acceder.
    - Que sean intuitivas, para que los usuarios se familiaricen rápidamente con ellas, no tengan dificultades durante su uso y que, además, no puedan hacerles cometer errores.
    - Que sean resistentes a los fallos de los usuarios.
    - Que cuenten con asistentes de ayuda que actúen como primer nivel de soporte a los usuarios.
    - Que los tiempos de conexión estén limitados y, pasado un tiempo de inactividad, se suspenda la sesión de los usuarios.
- **Mejorar las conexiones a Internet,** de forma que sean constantes y seguras, evitaría fallos de disponibilidad y situaciones de riesgo, ya que durante las averías o emergencias no se siguen los procedimientos habituales, y algunos controles de seguridad se obvian a favor de una resolución rápida de la incidencia.
- **Incorporar la gestión de la continuidad del negocio a los procedimientos habituales de actividad de la plataforma.** Se hace fundamental que tanto los centros educativos como las empresas de servicios tecnológicos cuenten con planes de contingencia en caso de caídas de la red, actos violentos o desastres naturales que puedan impedir un uso normal de la información y los sistemas. Estos planes de contingencia deberán estar dimensionados de acuerdo con las características de la plataforma y la infraestructura en la que se apoya. En

cualquier caso, deben tenerse en cuenta los recursos disponibles en cada organización para diseñarlos, de manera que sea factible llevarlos a cabo cuando sea necesario. Esto significa que no tienen que ser especialmente complejos o caros, sino que hay que valorar en cada caso las opciones disponibles. Por ejemplo, los colegios pueden establecer acuerdos entre ellos, de manera que, si uno se ve afectado por un incidente que ponga en peligro su continuidad, pueda utilizar las instalaciones de otro que no se haya visto afectado.

- **Gestionar los incidentes.** Son tan escasos, que las acciones realizadas para solucionarlos no se registran. Es importante que desde la Administración pública se mantenga una labor de vigilancia tecnológica a través de un registro de las incidencias para poder identificar vulnerabilidades, y de los mecanismos y convenios que esta pueda generar con las Fuerzas y Cuerpos de Seguridad para alertar y perseguir a los causantes de dichos incidentes. Esto no exime a las propias plataformas de tener un registro de las vulnerabilidades. Para poder hacerlo de manera coherente, los centros educativos deberían tener mecanismos para que tanto los alumnos como el personal docente o administrativo pudieran informar de incidentes potencialmente dañinos. Tal vez así se pongan al descubierto muchos incidentes que ahora pasan inadvertidos. Por otro lado, los administradores de los sistemas deben tener también sus propios mecanismos para informar a quien esté capacitado para solucionarlos, y procedimientos formales para detectar y gestionar incidentes de seguridad y fallos de los sistemas de información. Deben existir procedimientos formales que permitan hallar la solución a los problemas que ocurran, estudiando las causas que los hayan originado para así eliminarlos eficazmente.

6.5 Seguridad de contenidos

- **Impulsar, mediante la concesión de créditos o exenciones fiscales, la implantación de las soluciones necesarias para garantizar la seguridad informática.** Dados los enormes costes que la implantación, mantenimiento y certificación conllevan, se ha de primar la seguridad a los contenidos frente a los costes de los mismos que tienen para los desarrolladores de las plataformas.

- **Contar con políticas y directrices de seguridad en los centros educativos y en los organismos o empresas que soportan las infraestructuras de dichos centros.** De esta manera, se conseguiría unificar y mejorar las prácticas de los usuarios, manteniendo al menos un nivel mínimo aceptable de seguridad en ellos. Estas políticas deben especificar el mecanismo sancionador que se pondría en marcha en caso de infracciones a dicha política.

- **Asignar recursos humanos a las tareas de seguridad.** Esto debe hacerse en diversas categorías:

    - En la de dirección y supervisión. Debe haber personas que sean capaces de coordinar las diversas tareas y conseguir que los criterios establecidos se cumplan. Hay que cubrir también el papel de interlocutor entre los diversos implicados; es decir, desde el sector educativo, es necesario que haya alguien que comprenda las necesidades educativas y sus implicaciones tecnológicas, y sea capaz de trasladarlas a quienes desarrollan o mantienen las plataformas para que estas den un servicio adecuado.

        - Desde el lado de los desarrolladores o los proveedores de plataformas, es necesario que haya alguien capaz de entender los requisitos tanto funcionales como técnicos, organizativos, pedagógicos, de facilidad de uso y de seguridad que presenta una aplicación que se va a utilizar en un entorno tan especial, para que pueda colaborar en el diseño de una plataforma que cubra las expectativas de todos los usuarios.

        - En el caso de los entes públicos, es fundamental contar con una figura (al estilo de la labor que desempeñan los coordinadores TIC en los centros educativos) o una entidad que pueda materializar, en requisitos y programas coherentes, las necesidades de la comunidad educativa en el contexto de la Sociedad de la Información en la que hay que educar a los menores.

    - En la de ejecución. Es importante contar con recursos suficientes para llevar a cabo las numerosas tareas relacionadas con un uso seguro de las plataformas: la formación e información a los usuarios, el mantenimiento de las aplicaciones, la administración de los sistemas, la definición y actualización de las políticas de seguridad, etc.

- **Llevar a cabo análisis de riesgos.** Estos análisis deberían realizarlos, en primer lugar, los proveedores de plataformas, para incorporar a sus productos medidas de seguridad encaminadas a reducir los riesgos detectados. Los encargados de realizar las compras de estas aplicaciones deberían hacerlo también para exigir los correspondientes controles de seguridad, y poder tomar una decisión con criterio y en perspectiva global sobre cuál es el mejor producto para su situación.

- **Controlar los ataques de código malicioso.** A pesar de que las plataformas cuentan con entornos de operación y utilización muy cerrados, no son inmunes a

un posible ataque de código malicioso en cualquier formato (virus, gusanos, troyanos, etc.) Dado que la propagación de virus y otros riesgos es muy rápida, a menudo, sin que los usuarios finales sean conscientes de ello, es muy importante que las plataformas tengan un sistema de alerta de aviso rápido o, en su defecto, que cuenten con profesionales que lleven a cabo una supervisión constante, de manera que un incidente de este tipo no pasara inadvertido. En este punto, es fundamental que existan recursos humanos y técnicos suficientes y capaces de llevar a cabo de manera regular las siguientes acciones:

- Instalación y actualización de los programas de detección y eliminación de código malicioso.
- Revisión periódica del *software*.
- Actualización de la información.
- Filtración de contenidos inapropiados o de código malicioso en origen, evitando que sean los centros educativos los encargados de llevar a cabo esta labor.

Si no es así, puede que un ataque tenga éxito el tiempo suficiente para causar daños irreparables en los sistemas y la información que albergan.

- **Realizar de manera rigurosa y periódica copias de seguridad,** comprobándolas regularmente para verificar que son correctas. Debe almacenarse en estas copias toda la información necesaria para poder continuar dando servicio en caso de perderla. Debe determinarse una frecuencia razonable para que la pérdida de información sea mínima y establecer una segunda ubicación para que la copia no se vea afectada en caso de que algo suceda en las instalaciones donde están los equipos, es decir, debe estar físicamente alejada de estos. Cuando los datos y aplicaciones están centralizados, es relativamente sencillo mantener toda la información controlada y realizar la copia de seguridad de la información relevante. En el caso opuesto, cuando la información no está centralizada, hay que instaurar políticas de copias de seguridad a distintos niveles: administrador, operario, usuario, etc. Esto debe hacerse de manera que ninguna información relevante quede sin copia.

- **Gestionar la seguridad de la red.** Las plataformas suelen contar con una infraestructura de red compleja, con multitud de transacciones electrónicas soportadas por ella a diario. Es fundamental que se apliquen controles de red suficientes para garantizar la seguridad de la información que se transmite por ellas; por ejemplo: métodos de autenticación de usuarios, control de las conexiones a la red, criptografía, detección de intrusos y cortafuegos. Su buen

uso y disponer de una red centralizada de servicios proporcionados por la Administración pública ofrecen un nivel de seguridad con garantías y homogéneo para toda la comunidad educativa que abarca su ámbito de actuación y que no puede ser conseguido con iniciativas individuales por falta de medios técnicos y personal cualificado.

- **Realizar y gestionar auditorías de seguridad.** Este tipo de auditorías genera mucha información relevante en cuanto al estado técnico de los sistemas y puede detectar problemas latentes que de otro modo no saldrían a la luz. Asimismo, deberían sistematizarse para garantizar su seguimiento con independencia de las personas asignadas a su cometido.

- **Mejorar la autenticación e identificación segura de usuarios,** para que los problemas relacionados con el "préstamo" u olvido de contraseñas se eliminaran y hubiera más motivos para confiar en la identidad virtual de cada uno, de manera que se utilizaran más funciones con más asiduidad. Esto puede hacerse cambiando el habitual método de usuario y contraseña por otros sistemas más seguros para acceder a las aplicaciones, como los dispositivos biométricos, o bien reforzándolos, por ejemplo, utilizando firmas digitales.

ANEXO I: ENTIDADES ENTREVISTADAS

I Administraciones públicas

- **Agencia Española de Protección de Datos:** María José Blanco Antón (subdirectora general del Registro General de Protección de Datos).
- **BECTA:** Vanesa Pittard (directora de E-strategy).
- **Centro Nacional de Información y Comunicación Educativa (CNICE):** Juan José Blanco (jefe del Servicio de Medios Tecnológicos) y Juan Pérez (jefe del Servicio de Telemática y Desarrollo).
- **INTECO:** Marcos Gómez Hidalgo (subdirector de e-confianza de INTECO), Pablo Pérez San-José (gerente del Observatorio de la Seguridad de la Información) y Javier Rey Perille (técnico del Observatorio de la Seguridad de la Información).
- **Red.es:** Juan Ramón González y María Dolores Gonzalo (coordinadores de Aplicaciones, Formación y Contenidos).

II Consejerías de educación

- **Andalucía:** Rafael García (director del Centro de Gestión Avanzado).
- **Castilla y León:** María José Martínez y Javier Fernández (responsables de Contenidos de la Plataforma de CyL).
- **Cataluña:** Jordi Vivancos (responsable de Proyectos TIC para Educación), Laia Martui (Soporte Legal), Jordi Orgue (responsable de Sistemas del Área TIC), Dolors Jiménez (responsable de Calidad del Área TIC) y Assumpta Rocosa (directora del Área TIC).
- **Extremadura:** Vicente Parejo (coordinador TIC) y Jesús Francisco Morcillo (responsable de Sistemas).
- **Madrid:** Felipe Retortillo (jefe de Dirección de Desarrollo de Nuevas Tecnologías y responsable de la Plataforma EducaMadrid).

III Desarrolladores de plataformas

- **Anaya:** Carlos San José (director del Departamento de Contenidos y Servicios en Red).
- **Cospa-Agilmic:** Ignasi Hosta (director comercial) y Xavi Valls (gerente de Sistemas).

- **Divisa IT:** David Rodríguez (director de Tecnología).
- **Grupo Gesfor:** José Ruiz (subdirector de Seguridad y Open-Source).
- **Grupo SM:** José Luis Pastor (gerente de Sistemas de la Información).
- **Intel Skoool:** Juan Pablo Ferrero (director de Desarrollo de la Sociedad de la Información de Intel España) y Enrique Celma (director del Sector de Educación).
- **Santillana:** Juan Carlos Bermejo (gerente de Tecnología).

IV Empresas de seguridad informática

- **S21 SEC:** Antonio Ramos (director de Normativa y Buenas Prácticas) y Alfonso del Castillo (director del Área de Tecnología de la Seguridad y de la Seguridad Gestionada).

V Asociaciones

- **Asociación Protégeles:** Guillermo Cánovas (presidente).
- **Confederación Española de Asociaciones de Padres de Alumnos (CEAPA):** Pedro Rascón (vicepresidente).
- **Escuelas Católicas:** Alberto Mayoral (responsable TIC).
- **ISACA:** Fernando Hervada (presidente 2004-2006).
- **ISMS Forum Spain:** Gianluca d'Antonio (presidente).

VI Profesores, padres y alumnos

- María Paz Arriaza (madre de alumnos de Primaria).
- Javier Antonio Puente (coordinador TIC del IES Doña Jimena de Gijón).
- Grupo de alumnos del Colegio Nuestra Señora de Lourdes de Valladolid.

VII Otros

- **Brigada de Investigación Tecnológica de la Policía Nacional:** Manuel Vázquez López (comisario-jefe de la Brigada de Investigación Tecnológica).
- **Grupo de Delitos Telemáticos de la Guardia Civil:** Juan Salom (comandante jefe).

- **Universitat Oberta de Catalunya (UOC):** Magí Almiral (director de Tecnología Educativa) y Frances Rubirosa (responsable de Seguridad Tecnológica).

ANEXO II: LEGISLACIÓN RELEVANTE

I Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)

Esta ley se complementa con el reglamento estipulado en el Real Decreto 1720/2007.

La LOPD es de aplicación a los datos de carácter personal registrados en soporte físico (incluye el papel) que los haga susceptibles de tratamiento, y su uso posterior por sectores públicos y privados.

Su objetivo es garantizar y proteger, en lo concerniente al tratamiento de los datos personales (automatizados o no), las libertades públicas y los derechos fundamentales de las personas físicas, y, especialmente, de su honor e intimidad personal y familiar.

El personal que tenga acceso a estos datos está obligado al secreto profesional respecto a ellos y, por tanto, no se comunicarán datos a terceras personas para un fin distinto de aquel para el que fueron recabados.

Asimismo, el personal deberá mantener en las bases de datos la información necesaria para el desarrollo de sus funciones, es decir, que no deben ser excesivos en relación con el ámbito y las finalidades determinadas. Los datos de carácter personal serán exactos y puestos al día, de forma que respondan con veracidad a la situación actual del afectado.

Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

- De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información.
- Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Con el fin de mantener la confidencialidad, integridad y disponibilidad de la información, la LOPD exige la existencia de un documento de seguridad con las normas y procedimientos para cumplir los puntos anteriores.

Los afectados, personas de las que se almacenan datos de carácter personal, tienen una serie de derechos amparados por esta ley.

- **Derecho de información.** Cuando el afectado proporciona sus datos, debe ser informado de lo expuesto en los puntos anteriores.

- **Derecho de acceso, cancelación, rectificación y oposición.** El afectado puede ver la información que se dispone de él, cambiar esos datos para que sean correctos y exactos, cancelar la información que se almacene de él y oponerse a que se almacene, en este caso, con perjuicio de la funcionalidad para la que fueron recabados.

II Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones

Es una ley que incorpora al ordenamiento jurídico español el contenido de la normativa comunitaria, respetando plenamente los principios recogidos en ella, aunque adaptándolos a las peculiaridades propias del derecho y la situación económica y social de nuestro país.

El objeto de esta ley es la regulación de las telecomunicaciones, que comprenden la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas y los recursos asociados, de conformidad con el artículo 149.1.21ª de la Constitución.

Los objetivos y principios de esta ley son, entre otros, los siguientes.

- Fomentar la competencia efectiva en los mercados de telecomunicaciones.

- Garantizar el cumplimiento de las referidas condiciones y de las obligaciones de servicio público en la explotación de redes y la prestación de servicios de comunicaciones electrónicas.

- Promover el desarrollo del sector de las telecomunicaciones.

- Hacer posible el uso eficaz de los recursos limitados de telecomunicaciones.

- Defender los intereses de los usuarios, asegurando su derecho al acceso a los servicios de comunicaciones electrónicas en adecuadas condiciones de elección, precio y calidad, y salvaguardar, en la prestación de estos, la vigencia de los imperativos constitucionales, en particular, el de no discriminación; el del respeto a los derechos al honor, a la intimidad, a la protección de los datos personales y al

secreto en las comunicaciones; el de la protección a la juventud y a la infancia, y la satisfacción de las necesidades de los grupos con privaciones especiales, tales como las personas con discapacidad. A estos efectos, podrán imponerse obligaciones a los prestadores de los servicios para la garantía de dichos derechos.

- Fomentar, en la medida de lo posible, la neutralidad tecnológica en la regulación.
- Promover el desarrollo de la industria de productos y servicios de telecomunicaciones.
- Contribuir al desarrollo del mercado interior de servicios de comunicaciones electrónicas en la Unión Europea.

III Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico

Regula el régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios y a los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones. Incluye asimismo las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia, y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

Esta ley será de aplicación a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos.

IV Ley 59/2003, de 19 de diciembre, de Firma Electrónica

Regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

Se aplicará a los prestadores de servicios de certificación establecidos en España y a los servicios de certificación que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España. Se denomina prestador de servicios de certificación a la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

La firma electrónica avanzada es aquella que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere, y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

La firma electrónica reconocida tendrá, respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel.

Se considera documento electrónico el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente.

La firma electrónica es uno de los mecanismos de autenticación que los entrevistados han mencionado como posibles sustitutos al tradicional usuario-contraseña. Por otro lado, dado el mencionado aumento de servicios y comunicaciones, utilizar la firma electrónica en la transmisión de información sería un método efectivo de garantizar su seguridad.

V Real Decreto Legislativo 1/1996, de 12 de abril, de Ley de Propiedad Intelectual

Esta ley establece que la propiedad intelectual de una obra literaria, artística o científica corresponde al autor por el solo hecho de su creación.

La propiedad intelectual está integrada por derechos de carácter personal y patrimonial, que atribuyen al autor la plena disposición y el derecho exclusivo a la explotación de la obra, sin más limitaciones que las establecidas en la ley.

Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre otras las siguientes.

- Los libros, folletos, impresos, epistolarios, escritos y discursos.
- Conferencias, informes forenses, explicaciones de cátedra y cualesquiera otras obras de la misma naturaleza.
- Los proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería.
- Los gráficos, mapas y diseños relativos a la topografía, la geografía y, en general, a la ciencia.

- Las obras fotográficas y las expresadas por procedimiento análogo a la fotografía.
- Los programas de ordenador.

El título de una obra, cuando sea original, quedará protegido como parte de ella.

Sin perjuicio de los derechos de autor sobre la obra original, también son objeto de propiedad intelectual:

- Las traducciones y adaptaciones.
- Las revisiones, actualizaciones y anotaciones.
- Los compendios, resúmenes y extractos.
- Cualesquiera transformaciones de una obra literaria, artística o científica.

También son objeto de propiedad intelectual en los términos del libro I de la presente ley las colecciones de obras ajenas, de datos o de otros elementos independientes como las antologías y las bases de datos que por la selección o disposición de sus contenidos constituyan creaciones intelectuales, sin perjuicio, en su caso, de los derechos que pudieran subsistir sobre dichos contenidos.

La protección reconocida en el presente artículo a estas colecciones se refiere únicamente a su estructura en cuanto a la forma de expresión de la selección o disposición de sus contenidos, no siendo extensiva a estos.

A efectos de la presente ley, y sin perjuicio de lo dispuesto en el apartado anterior, se consideran bases de datos las colecciones de obras, de datos o de otros elementos independientes dispuestos de manera sistemática o metódica, y accesibles individualmente por medios electrónicos o de otra forma.

La protección reconocida a las bases de datos en virtud del presente artículo no se aplicará a los programas de ordenador utilizados en la fabricación o en el funcionamiento de bases de datos accesibles por medios electrónicos.

Este es un asunto en el que muchos implicados reconocen que existe un problema que, al no resultar en incidencias graves, permanece latente y en muchos casos ignorado. La facilidad para localizar y copiar información en formatos digitales hace que se infrinja esta ley de manera habitual y cotidiana, a veces, de manera involuntaria, simplemente por desconocimiento de que la información utilizada está sujeta a los derechos de propiedad intelectual. Esto es particularmente serio en el caso del personal docente, que es el mayor consumidor y productor de contenidos.

VI Ley 17/2001, de 7 de diciembre, de Propiedad Industrial

Para la protección de los signos distintivos se concederán, de acuerdo con la presente ley, los siguientes derechos de propiedad industrial.

- Las marcas.
- Los nombres comerciales.

La solicitud, la concesión y los demás actos o negocios jurídicos que afecten a los derechos señalados en el apartado anterior se inscribirán en el Registro de Marcas, según lo previsto en esta ley y en su reglamento.

El Registro de Marcas tendrá carácter único en todo el territorio nacional y su llevanza corresponderá a la Oficina Española de Patentes y Marcas, sin perjuicio de las competencias que en materia de ejecución de la legislación de propiedad industrial corresponden a las comunidades autónomas, según se desarrolla en esta ley.

El derecho de propiedad sobre la marca y el nombre comercial se adquieren por el registro válidamente efectuado de conformidad con las disposiciones de la presente ley.

Esta ley tiene el problema expresado anteriormente para la propiedad intelectual. Los productores de contenidos ignoran los requisitos de esta ley y utilizan indebidamente marcas y nombres comerciales, lo cual puede acabar en una demanda de la empresa afectada.

VII Ley 20/2003, de 7 de julio, de Protección Jurídica del Diseño Industrial

Esta es una ley que tiene por objeto establecer el régimen jurídico de la protección de la propiedad industrial del diseño.

Todo diseño que cumpla los requisitos establecidos en esta ley podrá ser protegido como diseño registrado mediante su inscripción, válidamente efectuada, en el Registro de Diseños.

La solicitud, la concesión y los demás actos o negocios jurídicos que afecten al derecho sobre el diseño solicitado o registrado se inscribirán en el Registro de Diseños, según lo previsto en esta ley y en su reglamento.

El Registro de Diseños tendrá carácter único en todo el territorio nacional y su llevanza corresponderá a la Oficina Española de Patentes y Marcas, sin perjuicio de las competencias que en materia de ejecución de la legislación de propiedad industrial corresponden a las comunidades autónomas, según se establece en esta ley.

VIII Ley 30/2007, de 30 de octubre, de Contratos del Sector Público

La presente ley tiene por objeto regular la contratación del sector público, a fin de garantizar que la misma se ajusta a los principios de libertad de acceso a las licitaciones, publicidad y transparencia de los procedimientos, y no discriminación e igualdad de trato entre los candidatos, y de asegurar, en conexión con el objetivo de estabilidad presupuestaria y control del gasto, una eficiente utilización de los fondos destinados a la realización de obras, la adquisición de bienes y la contratación de servicios mediante la exigencia de la definición previa de las necesidades a satisfacer, la salvaguarda de la libre competencia y la selección de la oferta económicamente más ventajosa.

Es igualmente objeto de esta ley la regulación del régimen jurídico aplicable a los efectos, cumplimiento y extinción de los contratos administrativos, en atención a los fines institucionales de carácter público que a través de los mismos se trata de realizar.

IX Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor

Esta ley ofrece un amplio marco jurídico de protección al menor que vincula a todos los poderes públicos, a las instituciones específicamente relacionadas con los menores, a los padres y familiares, y a los ciudadanos en general.

Los derechos de los menores que contempla la ley son:

- Los que les reconocen la Constitución y los tratados internacionales de los que España sea parte. Los poderes públicos garantizarán el respeto de los derechos de los menores y adecuarán sus actuaciones a la presente ley y a la mencionada normativa internacional.

- Derecho al honor, a la intimidad y a la propia imagen. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones, la difusión de información o la utilización de imágenes o nombre de los menores en los medios de comunicación. Los padres o tutores y los poderes públicos respetarán estos derechos y los protegerán frente a posibles ataques de terceros.

- Derecho a la información. Los menores tienen derecho a buscar, recibir y utilizar la información adecuada a su desarrollo. Los padres o tutores y los poderes públicos velarán por que la información que reciban los menores sea adecuada, y las administraciones públicas incentivarán la producción y difusión de materiales informativos y facilitarán el acceso de los menores a los servicios de información.

- Libertad ideológica. El menor tiene derecho a la libertad de ideología, conciencia y religión. Los padres o tutores tienen el derecho y el deber de cooperar para que el menor ejerza esta libertad de modo que contribuya a su desarrollo integral.

- Derecho de participación, asociación y reunión. Los menores tienen derecho a participar plenamente en la vida social, cultural, artística y recreativa de su entorno.

- Derecho a la libertad de expresión. Los menores gozan del derecho a la libertad de expresión en los términos constitucionalmente previstos, incluyendo la publicación y difusión de sus opiniones, la edición y producción de medios de difusión, y el acceso a las ayudas que las administraciones públicas establezcan con tal fin.

- Derecho a ser oído. El menor tiene derecho a ser oído, tanto en el ámbito familiar como en cualquier procedimiento administrativo o judicial en que esté directamente implicado y que conduzca a una decisión que afecte a su esfera personal, familiar o social.

La Ley del Menor es una fuente importante de requisitos para las plataformas digitales. Deben estar diseñadas, desarrolladas, implantadas y gestionadas de manera que se garanticen los derechos reflejados en esta ley. Por otro lado, es una oportunidad para los desarrolladores, la Administración y los gestores de los centros para impulsar los nuevos usos de las TIC en la enseñanza, abriendo nuevos modos de docencia que posibiliten que el menor realmente ejerza sus derechos en un entorno seguro.

ANEXO III: REFERENCIAS BIBLIOGRÁFICAS

I Administración pública

- Agencia Española de Protección de Datos (2006): *Plan sectorial de oficio a la enseñanza reglada no universitaria*. Madrid, AEPD.
- Agencia Española de Protección de Datos (2008): *Documento de trabajo 1/08 sobre la protección de datos personales de los niños (directrices generales y el caso especial de los colegios)*. En línea. Disponible en https://www.agpd.es/upload/Canal_Documentacion/Internacional/wp_29/menores_es.pdf
- BECTA, ICT (2004): *Essential guides for school governors safety and security with ICT*.
- BECTA: http://www.becta.org.uk/research
- BECTA (2006): *Learning platform functional requirements*. Versión 1.
- BECTA (2006): *Learning platform technical specifications*. Versión 1.
- BECTA (2008): *Safeguarding children in a digital world. Developing an LSCB e-safety strategy*.
- EUROPEAN COMMISSION (1996): *Informe: el multimedia educativo*. Luxemburgo: Commission Européenne. En línea. Disponible en http://www.echo.lu
- EUROPEAN COMMISSION (2000): *Informe: e-learning; concebir la educación del futuro*. Luxemburgo: Commission Européenne.
- EUROPEAN COMMISSION: *Proyecto Safer Internet Plus*. En línea. Disponible en http://ec.europa.eu/information_society/activities/sip/index_en.htm
- EUROPEAN COMMISSIO: *E-learning program*. En línea. Disponible en http://ec.europa.eu/education/archive/elearning/index_en.html
- EUROPEAN COMMISSION: *eTwinning*. En línea. Disponible en http://www.etwinning.net/ww/en/pub/etwinning/
- EUROPEAN COMMISSION *European Computer Driving License Programme*. En línea. Disponible en http://www.ecdl.com/publisher/index.jsp

- EUROPEAN COMMISSION Directorate-General Information Society and Media (2007): *Safer Internet For Children Qualitative Study In 29 European Countries - National Analysis: Spain*. Abril.

- FEDERAL OFFICE FOR INFORMATION SECURITY (BSI) (2004): *The IT Baseline Protection Manual*. En línea. Disponible en http://www.bsi.bund.de/english/gshb/manual/download/pdfversion.zip

- INTECO: *"Estudio sobre la seguridad de la información y e-confianza de los hogares españoles. Primera oleada (diciembre de 2006-enero de 2007)*. En línea. Disponible en http://www.observatorio.inteco.es

- INTECO *Estudio sobre la seguridad de la información y e-confianza de los hogares españoles. Tercera oleada (mayo-julio de 2007)*. En línea. Disponible en http://www.observatorio.inteco.es

- INTECO *Política de contraseñas y seguridad de la información*. En línea. Disponible en http://www.observatorio.inteco.es

- Red.es: *Informe sobre la implantación y uso de las TIC en los centros docentes de Educación Primaria y Secundaria (curso 2005-2006)*.

- Red.es: *Proyecto Internet en el Aula (2005-2008)*. http://www.red.es/actividades/internet_aula.html

- Red.es: *Proyecto Enseña (2007-2008)*. http://www.red.es/actividades/ensena.html

- Red.es y Centro Nacional de Información y Comunicación Educativa (CNICE) (2007): *Informe sobre la implantación y uso de las TIC en los centros docentes de Educación Primaria y Secundaria (curso 2005-2006)*. Madrid. En línea. Disponible en http://www.oei.es/TIC/DocumentoBasico.pdf

- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) (2008): *Estándares de competencia en TIC para docentes*. En línea. Disponible en http://cst.unesco-ci.org/sites/projects/cst/default.aspx

- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) (2008): *Policy Framework; Competency Standards Modules e Implementation Guidelines. ICT Competency Standards for Teacher*. En línea. Disponible en http://cst.unesco-ci.org/sites/projects/cst/The%20Standards%20SP/Forms/AllItems.aspx

- Universitat Oberta de Catalunya (UOC) (2004): *Formación universitaria y TIC: nuevos usos y nuevos roles*. En línea. Disponible en http://www.uoc.edu/rusc

II Asociaciones

- APCI Y PROTÉGELES (2002): *Seguridad infantil y costumbres de los menores en internet*. En línea. Madrid, El Defensor del Menor en la Comunidad de Madrid. Disponible en http://www.protegeles.com/costumbres.asp

- MAIL ABUSE PREVENTION SYSTEM (MAPS): *Asociación internacional de lucha contra el spam*. En línea. Disponible en http://www.mail-abuse.com/

III Estudios académicos

- CASEY, H.; HARRIS, J., Y RAKES, G. (2001): *Why change? Addressing Teacher Concerns toward Technology*.

- CHIANN-RU, S. (2002): "Literature review for hypermedia study from an individual learning differences perspective", en *British Journal of Educational Technology*, 33 (4), 435-447.

- FERRÁNDEZ, ADALBERTO (1996): "El formador en el espacio educativo de las redes", en *Educar*, 20, 43-67.

- GILL, T. (ed.) (1996): *Electronic children. How children are responding to the informations revolution*. Londres, National Children Bureau.

- IES DOÑA JIMENA (2007): *Informe de evaluación III: curso 2006-2007*. Adscrito al proyecto Centros de Uso Avanzado de las Tecnologías Educativas. Gijón, Asturias.

- JONES, A. (2004): *A review of the research literature on barriers to the uptake of ICT by teachers*. British Educational Communications and Technology Agency (BECTA).

- LAJOIE (2002): *Computers as cognitive tools*. Hillsdale, Erbaulm.

- LEE, C.; CHENG, Y.; RAI, S., Y DEPICKERE (2005): "What affect student cognitive style in the development of hypermedia learning system?", en *Computers & Education*, 45, 1-19.

- MARCHESI Y MARTÍN (2003): *Tecnología y aprendizaje. Investigación sobre el impacto del ordenador en el aula*. Grupo SM.

- MARQUÉS, P. (2005): *Las TIC y sus aportaciones a la sociedad*. UAB.

- NEGROPONTE, N. (1995): *El mundo digital*. Barcelona, Ediciones B.
- NEWHOUSE, P. (2002): *Literature review. The impact of ICT on learning and teaching*. Western Australia, Specialist Educational Services.
- SIGALES, C. (2004): *Formación Universitaria y TIC: nuevos usos y nuevos roles*. En línea. Disponible en http://www.uoc.edu/rusc/dt/esp/sigales0704.pdf

IV Legislación y normas

- Ley 17/2001, de 7 de diciembre, de Propiedad Industrial.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley 20/2003, de 7 de julio, de Protección Jurídica del Diseño Industrial.
- Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 30/2007, de 30 de octubre, de Contratos del Sector Público.
- Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1631/2006, de 29 de diciembre, por el que se establecen las enseñanzas mínimas correspondientes a la educación.
- Real Decreto Legislativo 1/1996, de 12 de abril, de Ley de Propiedad Intelectual.
- MAGERIT (2006): *Metodología de análisis y gestión de riesgos de los sistemas de información*. Ministerio de Administraciones Públicas, versión 2.0. En línea. Disponible en http://www.csi.map.es/csi/pdf/magerit_v2/metodo_v11_final.pdf
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2001): *NIST Handbook An Introduction to Computer Security. Special Publication 800-12*.
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2002): *Contingency Planning Guide for Information Technology Systems, SP 800-34 NIST*. En línea. Disponible en http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2006): *Guide for Developing Performance Metrics for Information Security, SP 800-80 NIST's Computer Security Division*, 4 de mayo. En línea. Disponible en http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-80

- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: AN INTRODUCTION TO COMPUTER SECURITY: *The NIST Handbook, Special Publication 800-12*.

V Proveedores de seguridad

- ÁLVAREZ, G., Y PÉREZ, P. (2004): *Seguridad informática para empresas y particulares*. McGraw-Hill.

- JUNGE, KERSTIN, Y HADJIVASSILIOU, KARI *(2007): What are the EU and member states doING TO address digiTAL LITERACY? E-learning Papers, núm. 6. ISSN 1887-1542.*

- *TELEFÓNICA DE ESPAÑA, GRUPO DE INVESTIGACIÓN CIVÉRTICE,* UNIVERSIDAD DE NAVARRA Y EDUCARED (2007): *Generaciones interactivas en Iberoamérica. Niños y adolescentes frente a las pantallas. Retos educativos y sociales*.

VI Metodología cualitativa

- ALONSO, L. E. (1998): *La mirada cualitativa en sociología*. Madrid, Fundamentos.

- FAGES, J. B. (1990): *Comunicación entre personas en grupo* (trad.), Toulouse. Privat.

- LESY, M. (1976): *Real Life: Louisville in the Twenties*. Nueva York, Pantheon.

- TAYLOR, S. J., Y BOGDAN, R. (1998): *Introducción a los métodos cualitativos de investigación*. Barcelona, Paidós.

- WAX, R., (1971): *Doing Fieldwork: Warnings and Advice*. Chicago, University of Chicago Press.

- WEBB, E.; CAMPBELL, D.; SCHWARTZ, R., Y GROVE J. (1996): *Nonreactive Measures in the Social Sciences*. Boston, Houghton Mifflin

ÍNDICE DE TABLAS

Instituto Nacional
de Tecnologías
de la Comunicación

http://www.inteco.es

http://observatorio.inteco.es