

NUEVO MODELO DE EVALUACIÓN ASISTIDA POR ORDENADOR EN EDUCACIÓN A DISTANCIA

(NEW MODEL OF COMPUTER-AIDED ASSESSMENT IN DISTANCE EDUCATION)

Rosario Gil Ortego

Manuel Castro Gil

Gabriel Díaz Orueta

Sergio Martín Gutiérrez

Elio San Cristóbal Ruiz

Universidad Nacional de Educación a Distancia, UNED (España)

RESUMEN

En la actualidad, en aras de buscar un medio para autenticar a los usuarios, se comprueba que los sistemas de acceso a la información junto con las tecnologías de las que se dispone comúnmente no aseguran la identidad de las personas que acceden. En general, aquellos recursos protegidos y solo accesibles a un público en concreto pueden seguir políticas de asignación de roles o gestión de accesos por parte de un administrador. Además, muchas páginas disponen de herramientas de auditoría por defecto, que si bien la privacidad de los usuarios se ve reducida, pueden monitorizar y trazar el rastro de acciones no permitidas.

Ante estas herramientas, queda pendiente asegurar la identidad del usuario. La investigación que se presenta en este artículo, tuvo como objetivo combinar las formas tradicionales de identificación con la autenticación por “*algo que se es*”. La experiencia se realizó en comunidades educativas dentro del ámbito de la universidad.

Palabras clave: característica biométrica, educación a distancia, evaluación, identificación.

ABSTRACT

Nowadays, we look for the perfect way to authenticate users but we have found that the systems of access to information along with the technologies that are commonly available do not ensure the identity of users. In general, those protected resources which can only be accessed by specific individuals, can be accessed by assigning roles or by an administrator who manages access to the system. In addition, many Webs have auditing tools by default. Auditing is a strong tool that lets us control the activities of the users. We can also trace actions not permitted. The inconvenience of this is the weak wall of privacy that users have.

Given these general tools, the issue at hand is how to ensure the identity of the users. The challenge of this project was to combine the traditional ways of authentication with authentication by *something uniquely personal to the user* within the online educational communities that are used in colleges.

Keywords: assessment, biometric, distance education, identification.

Las necesidades de la sociedad actual requieren de un aprendizaje continuo durante la vida laboral. Las enseñanzas, por tanto, evolucionan para ajustarse a lo que se reclama hoy en día. Ya no basta con el aprendizaje y evaluación continua sino que las características de la sociedad actual junto con la evolución de la tecnología hacia otras nuevas orienta la enseñanza en su conjunto hacia un aprendizaje que se pueda dar con libertad tanto en el tiempo como en cualquier lugar geográfico.

De esta evolución surge la educación a distancia y la educación combinada (b-learning o *blended learning*) como modalidades para cubrir las necesidades profesionales (Rama, 2010). La educación a distancia se vale de todos los medios tecnológicos existentes para diseñar y gestionar sus cursos. El uso de los sistemas de gestión de aprendizaje es bastante común en estas modalidades. Los sistemas de gestión de aprendizaje nos presentan cursos, talleres, test de evaluación y otros módulos educativos con el fin de dinamizar la enseñanza. Una idea tan simple como cambiar total o parcialmente (Henríquez Gabante y Ugel Garrido, 2012) el aprendizaje local y presencial a un medio más remoto entraña en verdad una compleja mecánica de gestión, además de nuevas amenazas que atentan contra el desarrollo normal y fluido de la enseñanza. En la investigación que ha dado lugar a este artículo nos centramos en las amenazas contra los modelos de aprendizaje a distancia, en concreto los temas concernientes a la identidad de los sujetos que acceden a los sistemas de gestión de aprendizaje.

Un acceso a los cursos controlado podría reducir el número de impostores o personas con intención maliciosa que manipulen contenidos o calificaciones. Se plantea por tanto el uso de tecnología identificativa que se pueda integrar en estos entornos. En esta investigación se hace un estudio de la misma, tomando como elección la técnica basada en lo que es o hace un sujeto; estas técnicas reciben el nombre de técnicas biométricas. La biometría está asociada generalmente a controles de acceso a instalaciones físicas pero también aparece en el control de redes. Su integración en e-learning es una iniciativa para aprovechar las ventajas y ubicuidad que da la educación a distancia, además de proporcionar una autenticidad en procesos de valor educativo como es la evaluación.

No se puede entender la educación como tal, ya sea a distancia o tradicional, si no va ligada a una evaluación y sus exámenes correspondientes. La evaluación (González y Gaudioso, 2006) de los estudiantes es una parte importante del sistema de enseñanza-aprendizaje. Por una parte, se necesita saber cuál es el conocimiento adquirido para actuar en consecuencia, y, por otra parte, los propios estudiantes necesitan conocer de manera objetiva el “saber” adquirido.

Por otra parte, la evaluación es uno de los puntos críticos de los programas de educación a distancia, por cuanto descansa en ella, por una parte, la credibilidad social de la certificación de los programas de e-learning, y por otra, la eficacia de los procesos de evaluación desplegados en los programas de e-learning.

PROBLEMA PLANTEADO

En orden a desarrollar una solución, en cuanto a seguridad en la evaluación, se presentan los entornos, donde dicho proceso se da en la UNED, y sus medidas contra cualquier amenaza realizadas. De igual forma, se muestra todo el abanico de entornos donde podría darse un proceso de evaluación mediante el uso de los sistemas de gestión de aprendizaje. De tal forma que, a través del hilo común del uso de la tecnología biométrica, nos damos cuenta de la problemática y debilidades en ciertos entornos que nos hace descartarlos como potenciales para su desarrollo.

OBJETIVO Y METODOLOGÍA DE TRABAJO

El objetivo de la investigación consistió en estudiar la implantación de la identificación biométrica en las aulas de examen. La metodología que se siguió fue la siguiente:

- Estudio de los diferentes entornos de evaluación: su problemática y soluciones que se plantean.
- Elección del entorno presencial.
- Análisis de las amenazas que existen en el entorno presencial.
- Prueba piloto en pruebas de laboratorio. Estudio de los resultados obtenidos y conclusiones.

ESTUDIO DE LOS DISTINTOS ENTORNOS DE EVALUACIÓN

A continuación se presentan los posibles escenarios que se generan por el mero hecho de trasladar la realización de los exámenes a un entorno Web controlado, ya sea ordenadores con acceso restringido en el laboratorio de la universidad o un recinto más vulnerable en cuanto a seguridad como puede ser un sitio público o el lugar de trabajo. En este punto no se trata de resolver todas las vulnerabilidades de estos nuevos escenarios, sino describirlos en sí y percibir esa necesidad de seguridad en la evaluación que se viene tratando.

Los exámenes en la UNED se realizan de forma presencial en los distintos centros habilitados. La estructura ramificada de la UNED da lugar a que el proceso de evaluación sea también distribuido. La realización de los exámenes por ordenador tiene de forma inmediata el beneficio de la eliminación de las copias de papel y todo el proceso administrativo que conlleva a la gestión de un examen.

El primer entorno será la realización de exámenes de forma presencial con ordenadores. No obstante, existen otros entornos que merecen nuestra atención. El entorno remoto proporciona una serie de beneficios respecto al anterior: evita posibles desplazamientos al centro asociado, la libertad de elegir el mejor momento para realizar un examen, y además, de cara a los administradores o examinadores, el mero hecho de no tener que controlar el recinto del examen ya es una ventaja. Como gran inconveniente, pero que a la vez sienta las bases del reto del examen a distancia, es el controlar este ambiente intrínsecamente inseguro.

Dentro de los entornos remotos estarían los remotos internos *en-casa* y los remotos externos *fuera-de-casa*. Los primeros tendrán un lugar fijo para todos los exámenes, a la vez será personal o propio, como la oficina o su casa. En este tipo de remotos se pueden estudiar las características del mismo e intentar hacer una generalización de ellos, así las aplicaciones o herramientas de seguridad utilizadas se podrán aplicar a todos los entornos remotos *en-casa*. El segundo tipo de remotos se define como un lugar cambiante, posiblemente en un lugar público como cibercafé o establecimientos con wireless. Este tipo de entornos resulta impensable a priori cómo poder controlarlos, ya sea por la tecnología actual que se posee o por la cantidad de eventos que pueden aparecer en estos ambientes. Encontrar una aplicación que pudiera ser aplicable en los *fuera-de-casa* sería verdaderamente una gran aportación, a la que se podrá llegar en base a pequeños avances.

Además de esta clasificación atendiendo al lugar donde se realiza el examen, dentro de cada grupo se puede hacer una segunda clasificación en función de las personas que intervienen: en examen individual o en grupo (normal o colaborativo).

Como última parte de esta clasificación (Gil y otros, 2008), es necesario tener en cuenta la presencia en los exámenes de documentación o material de apoyo y la no presencia del mismo (Figura 1).

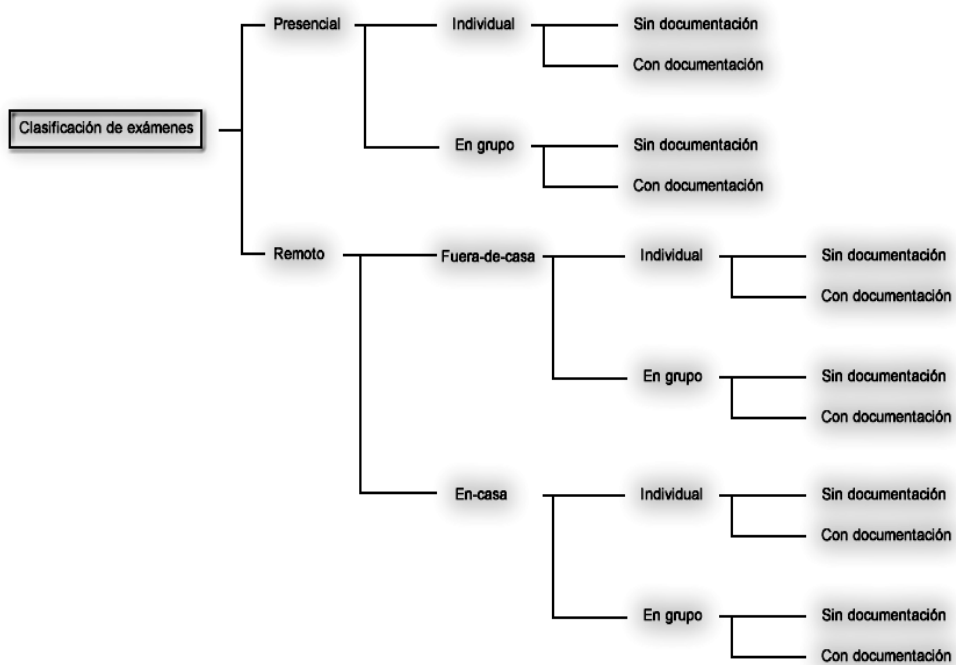


Figura 1. Tipos de entornos de evaluación

Examen presencial individual con y sin documentación

Proceso de realización de un examen:

- El estudiante se presenta en un centro asociado y se identifica ante un puesto de entrada compuesto por ordenador y lector de barras.
- El sistema valida que el estudiante puede realizar el examen por coincidencia de asignatura y hora.

- El sistema imprime una etiqueta, a recoger por el estudiante, donde muestra el puesto (fila y columna) donde se debe sentar en el aula de examen. El puesto estará dotado de un ordenador y un dispositivo biométrico.
- El ordenador identifica al estudiante y le muestra en pantalla el examen.
- El sistema de control de aula vigila el desarrollo adecuado del examen.
- Pasado el tiempo del examen, el estudiante o el sistema envía al profesor de la asignatura el examen cumplimentado.

Respecto al primer punto en la organización actual de la UNED, este proceso se realiza con un lector de código de barras donde el estudiante pasa su tarjeta de estudiante y se identifica para tener acceso al examen.

En el segundo paso del proceso, el mismo sistema utilizado en el punto anterior identifica la hora y la asignatura de la que se debe examinar el estudiante si es la que procede por el horario le da acceso al aula de examen. En este caso no sería necesario introducir ningún cambio respecto al modelo actual de *“valija virtual”*.

Una vez realizados los pasos uno y dos, el sistema saca por impresora el examen a realizar por el estudiante indicándole la fila y la columna donde se debe sentar en el aula de examen. En el sistema propuesto, el examen estará dentro de la plataforma educativa que use la universidad, por tanto, será accesible por ordenador en el aula de examen y la etiqueta impresa solo indicaría donde se debe sentar un estudiante. Por tanto el nuevo modelo exige la incorporación de un ordenador convencional o Table PC, por puesto, y una impresora de etiquetas para señalar el puesto del examinado. El sistema siguiendo la misma pauta actual impedirá que dos estudiantes de la misma asignatura se sienten juntos.

En el paso cuarto, una vez que el estudiante se ha sentado para realizar el examen, el ordenador con un control biométrico de acceso identifica que es el estudiante asignado por el sistema a ese puesto y le muestra el examen a realizar. De esta forma queda validada y comprobada la identidad del estudiante y por tanto no es necesaria ninguna identificación posterior, como se venía haciendo con el procedimiento de *“valija virtual”*.

En el quinto punto se aborda el sistema de control del comportamiento de los estudiantes para impedir la utilización de material inadecuado y/o la copia de

examen. Será necesario dotar al aula de examen de un puesto de control que se situará en un punto del aula donde el tribunal examinador tenga acceso para vigilar a los estudiantes y controlar la documentación que puede utilizar el estudiante. No obstante, esta configuración no exime al tribunal de realizar los controles que estime necesario.

En la última fase del proceso, el sistema controlará la duración individual de cada examen y avisará con antelación el término del mismo. Si el estudiante prorroga la duración del examen el sistema, con un margen previamente consensuado, cerrará la sesión enviando el examen al profesor de la asignatura. Todo el sistema debe contemplar la posibilidad de corte de energía eléctrica y operaciones inadecuadas del usuario realizando *backup* o copia de seguridad cada poco tiempo. Además, la impresión del examen completado y entrega a la salida del aula puede ser una prueba más de que los datos que ha introducido el estudiante permanecen inalterables y nadie los ha modificado.

En la figura 2 y 3 se muestra este potencial sistema de control en la evaluación presencial e individual.

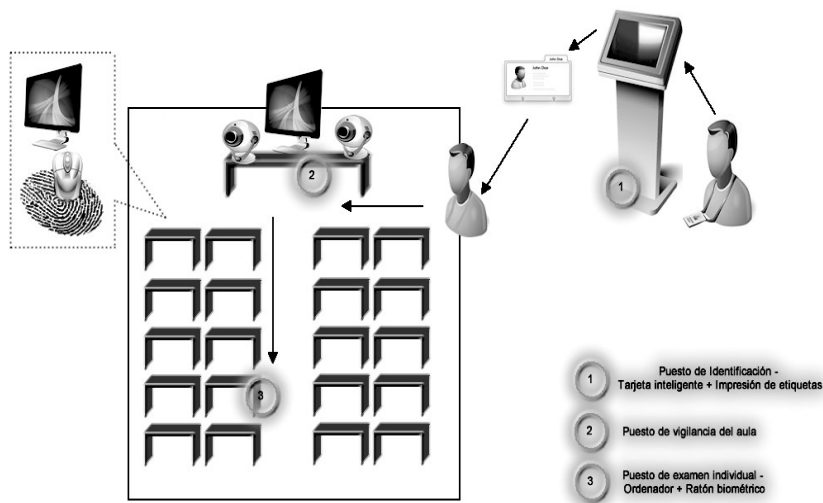


Figura 2. Esquema de un examen presencial individual con o sin documentación

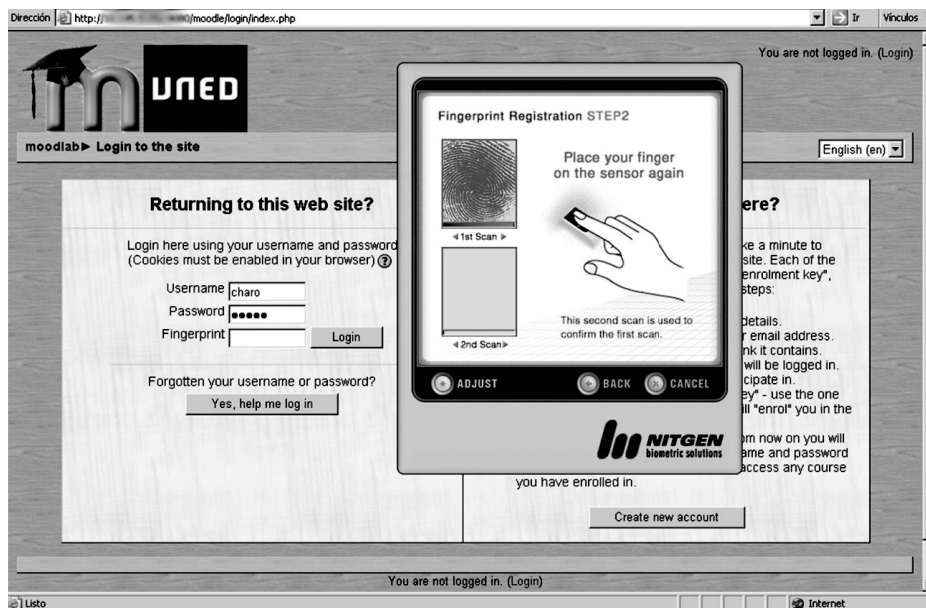


Figura 3. Control de acceso a la plataforma educativa, donde se realizará el examen, mediante verificación de la huella dactilar

En resumen, en el modelo propuesto los requerimientos del entorno serán los siguientes:

- Impresora de etiquetas indicando el puesto donde se debe sentar el estudiante.
- Cámaras para control del comportamiento del estudiante en el aula.
- Control de la identidad del examinado, uso de un dispositivo biométrico.
- Realización en aulas multimedia en los centros asociados o centros en el extranjero.
- Control del manejo o no de toda la documentación que se desee: libros, apuntes, etc.
- Envío por medio telemático del examen cumplimentado al profesor de la asignatura.

Problemas que se presentan:

- Una cuestión logística y coste de material: debe existir la disponibilidad de un ordenador o Table PC por estudiante presentado.
- Necesidad de conocimientos informáticos por parte del alumnado.
- En asignaturas técnicas existirá una complejidad al tener que utilizar fórmulas y/o símbolos.

Estos problemas están mediatizados tanto por el individuo que realiza el examen como por la institución.

Examen presencial en grupo con y sin documentación

En primer lugar, se debe aclarar la diferencia entre grupo y grupo colaborativo entendiéndose que el segundo se caracteriza por la asignación de roles a cada miembro del grupo. Las pruebas que se realizan en grupos son muy frecuentes tanto en entornos prácticos como en laboratorios donde se opta por una realización conjunta.

Proceso de realización de un examen:

- El estudiante se presenta en el laboratorio y se identifica ante un puesto de entrada compuesto por ordenador, lector de barras y lector biométrico.
- El sistema valida que el estudiante puede realizar el examen por coincidencia de asignatura y hora.
- Una base de datos local comprueba que el estudiante cumple los requisitos exigidos por el profesor de la asignatura y por tanto se puede examinar.
- La distribución y número de personas integrantes de cada grupo las fijará el profesor.
- El sistema de control de aula vigila el desarrollo adecuado del examen.

En este caso solamente será necesaria la identificación biométrica de cada asistente y el control mediante cámaras de un comportamiento adecuado del estudiante, por tanto, se necesitará un puesto de control en la entrada para realizar

dichas labores por el profesorado. No es necesaria la distribución automática de los estudiantes al ser un número reducido, y tampoco será necesario acceder a la plataforma educativa para realizar el examen ya que en entornos como laboratorios la tendencia es cumplimentar unas cuestiones referentes a la sesión de laboratorio. Sí deberá existir una base de datos local generada por el profesor de la asignatura que seleccione a los estudiantes que cumplan las condiciones para examinarse.

En el modelo propuesto los requerimientos del entorno serán los siguientes:

- Cámaras para control del comportamiento del estudiante en el aula.
- Control de la identidad del examinado.
- Control del manejo o no de toda la documentación que se desee: libros, apuntes, etc.

Problemas que se presentan:

- Excesivo tiempo de acceso para entrar a realizar el examen al existir un único puesto de control de entrada y realizarse la asignación de los puestos de forma manual.
- Aunque no es propiamente un problema, el sistema debe contemplar la posibilidad de emitir justificante de asistencia a la prueba. Dicho justificante se puede realizar en el puesto de control.

La imagen de todo este proceso de control se muestra en la figura 4.

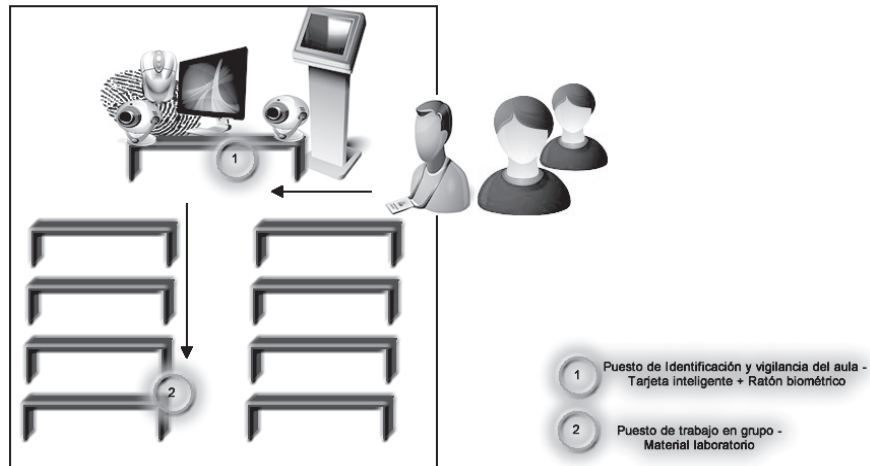


Figura 4. Esquema de un examen presencial en grupo con o sin documentación

Examen remoto en-casa e individual con y sin documentación

Aquí se abre un reto importante, este es: el control de eventos remotos. La evaluación no puede perder valía o seguridad en los resultados dependiendo del entorno que se elija.

El examen multimedia reducía en todo momento todo el papeleo y gestión de los mismos, por lo que también se utilizará en este nuevo entorno. De la misma forma, la identificación del individuo seguirá los pasos que los anteriores modelos de exámenes, es decir, mediante una verificación de una característica biométrica.

Pero sin apenas analizar este nuevo entorno, nos damos cuenta que con todo, esto no basta:

- ¿Cómo controlar que el individuo no sea suplantado después de la verificación inicial del examen?
- ¿Cómo controlar que no hay más personas en el recinto?
- ¿Cómo saber que no hace uso de otras aplicaciones con el ordenador?
- Uso de otros dispositivos tales como móviles, micrófonos, etc.

- Cuando la documentación no está permitida, ¿qué hacer?

Como primera medida para garantizar la identidad del usuario (Castro, Gil, Martín, Colmenar, Díaz y Peire, 2006) durante el examen se debe considerar, independientemente de lo que esté haciendo o de si está acompañado, la captura de una muestra biométrica en pequeños intervalos de tiempo, sin interferir en ningún momento en la tarea del examen. De esta forma ante cualquier cambio de identidad la aplicación se cerrará mostrando un mensaje previo con las causas de la clausura.

Como segunda consideración, se debe controlar el comportamiento del estudiante. Para ello se proponen los siguientes dispositivos ligados al funcionamiento de la aplicación:

- Aplicación cerrada, que no permita abrir ninguna otra ventana o aplicación que tenga como fin ayudar durante el examen.
- Control del audio del recinto mediante un micrófono de forma que se garantice que no se genera ningún ruido malicioso.
- Inhibidores de RF y de celulares, con lo que se evitará el uso de dispositivos que puedan facilitar la comunicación con alguien en el exterior.
- Control de proximidad o movimiento, lo que detectará si alguien ajeno al estudiante intenta moverse o desplazarse por el recinto.
- Control de la imagen, mediante una webcam, intentará completar el estudio del recinto de forma que se procure dar alcance a todos los flancos débiles de un examen a distancia.

La arquitectura, por tanto, será la mostrada en la figura 5.

El sistema de seguridad, como se puede observar, está compuesto por tres capas. La primera capa se desarrolla en el lado del usuario, es decir, del estudiante, y las dos últimas capas en el lado del servidor.

En la primera capa están todos los periféricos que analizan el entorno donde esté el estudiante realizando su examen. En esta capa, por tanto, estarán el micrófono, el inhibidor de RF y celular, el sensor de proximidad y la webcam. Además de estos periféricos se alojará también los propios para identificar al usuario, es decir, el

dispositivo biométrico, que en nuestro caso se trata de un ratón y el lector RFID (opcional). Cabe también decir que el navegador donde se mostrarán las preguntas del examen estará en esta capa.

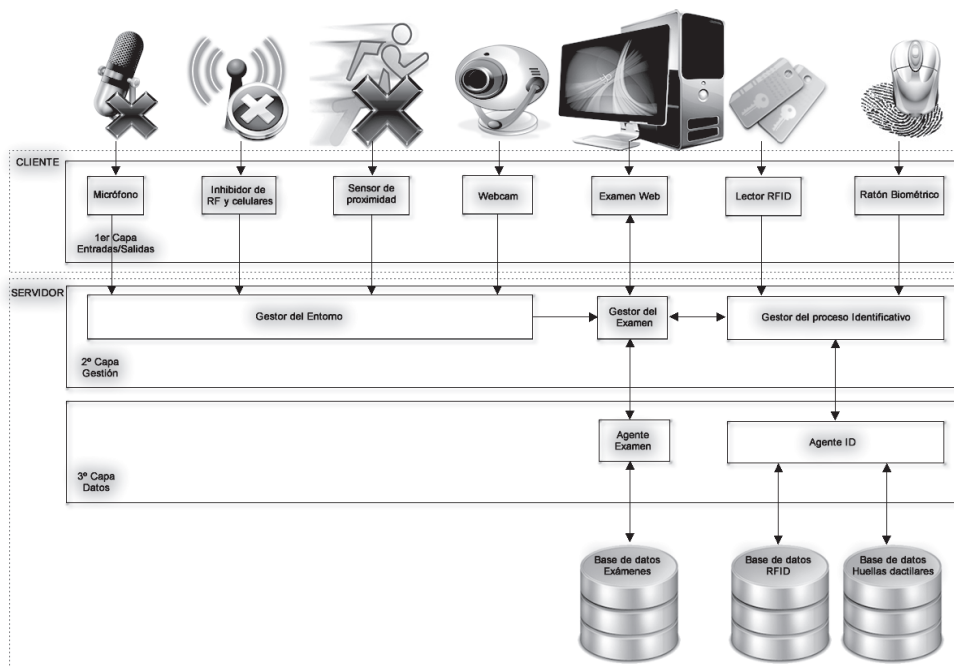


Figura 5. Arquitectura en un entorno remoto en-casa e individual

En la segunda capa habrá tres módulos que gestionarán respectivamente el entorno, el proceso mismo de examinarse y la identificación o verificación del usuario.

Por último, en la tercera capa estarán las tres tablas de la base de datos: para las huellas dactilares junto con sus datos personales (NIF, nombre, apellidos, etc.) y las asignaturas matriculadas; para IDs RFID (opcional) y si fuera necesario almacenar más datos de dispositivos; y, para las preguntas de los exámenes.

Según esta arquitectura nuestro sistema funcionaría de la siguiente forma:

- El proceso comienza cuando un usuario entra en la página web del examen en una comunidad educativa.

- Mediante el lector RFID (opcional) o el ratón biométrico se capturarán el ID y la huella dactilar y se enviarán ambos datos al módulo *Gestor del proceso Identificativo*.
- El módulo *Gestor del proceso Identificativo* decidirá si los datos son correctos o no preguntando al módulo *Agente ID*, el cual comparará la recién capturada huella dactilar y el ID RFID (opcional) en sus respectivas tablas de la base de datos.
- Si el usuario es aceptado se llamará al módulo *Gestor de Exámenes* a través del módulo *Gestor del proceso Identificativo*. El módulo *Gestor de Exámenes* se encarga de facilitar un específico examen para cada estudiante que accede a la aplicación. Nótese que el comportamiento entre gestores es genérico a cualquier sistema de gestión de aprendizaje; si particularizamos por ejemplo en Moodle (Moodle, 1999), una vez que el usuario es identificado en las tablas de identificación de usuarios de Moodle (*mdl_user*) e identificado respecto a su huella como un campo más dentro de una tabla de Moodle o generando una base de datos externa a Moodle, el usuario accederá a sus cursos en Moodle. Será el usuario el que acceda al examen del curso correspondiente del cual debe realizar una prueba.
- Durante toda la duración del examen los distintos dispositivos procurarán controlar todos los eventos que se produzcan en el recinto. Estos dispositivos, como ya dijimos, son: un micrófono, un inhibidor de RF y celular, un sensor de proximidad y una webcam.
- El módulo *Gestor del Entorno* controlará todos estos periféricos. Cuando alguno de ellos avise de un comportamiento extraño por parte del estudiante el módulo *Gestor de Exámenes* se encargará de cerrar la aplicación del examen.
- Finalmente, cuando el estudiante termine su examen, si no ha habido ningún problema se enviarán las respuestas al servidor el cual ya se encargará de corregirlo.
- Este diseño entraña una serie de problemas nuevos. Lo primero que nos podemos preguntar es: en qué momento se va a realizar la instalación de todos estos dispositivos y por quién. Además el gasto que supone un kit de estos para cada estudiante.

- La instalación es obvio que se debe realizar antes del periodo de exámenes, además, deberá realizarla un personal habilitado para tal función con el fin de evitar que el estudiante lo instale de forma involuntaria o a propósito incorrectamente.
- El coste es algo que debe hacer frente la propia universidad, y este podría elevarse de forma desmesurada si se integra en todos los estudiantes matriculados. Una opción de estos exámenes sería que tan solo se dieran cuando hubiera problemas de desplazamiento al centro asociado o extranjero más cercano. Serviría para aquellas personas discapacitadas, las que estuvieran en la cárcel o en un país extranjero bastante alejado del centro más próximo. Por supuesto, también se podría incluir a aquellos trabajadores con un estricto horario laboral y que no pudieran acudir en la fecha fijada por la universidad al centro asociado. Si tan solo se aplica a estas situaciones el gasto se vería reducido.
- La última consideración será plantearse un límite en la seguridad que queramos aplicar. Ya que en los “*en-casa*” estamos llevando el material a la propia casa o un lugar fijo donde pasa largo tiempo al día el estudiante y que pertenece al espacio personal de él, esta tecnología será intrusiva en todos estos recintos.
- Sobre el tema de la documentación, es cierto que las Webcams nos pueden decir si está consultando algún tipo de libro o apunte. Pero aún reduciendo el colectivo de personas que realicen esta modalidad de examen, hay una gran cantidad de imágenes a procesar. Lo que a priori exigiría un sistema de procesamiento de imágenes. Si este sistema se implementara el control de la documentación podría hacerse una realidad.

Examen remoto en-casa en grupo con y sin documentación

El entorno remoto se plantea como una posible solución para mitigar los problemas de movilidad o desplazamiento que se pueden presentar en un individuo, ya sea por problemas geográficos, minusvalía o cualquier otro tipo de impedimento.

Como se comentó, la modalidad de hacer un examen en grupo suele ajustarse a prácticas de laboratorio o exámenes de discusión. De esta forma un examen remoto en grupo independientemente de ser *en-casa* o *fuera-de-casa* debería ajustarse a un perfil de no movilidad y para exámenes de laboratorio.

Para el caso de un individuo con problemas de movilidad la solución para hacer un examen en grupo sería escoger a compañeros sin esta problemática y que pudieran

desplazarse al domicilio del primero, el cual estaría dotado de los medios que se han visto en el punto anterior.

La identificación sería de nuevo mediante características biométricas de todos los individuos del grupo y además habría que dotar la sala de sensores térmicos para calcular el número de personas, de forma que no pudiera exceder el número fijado para el grupo.

Los inhibidores de radio frecuencia y de celulares seguirían teniendo importancia en este entorno. Además, el bloqueo de otras aplicaciones en el ordenador.

El audio ya no tendría sentido controlarlo, debido, como ya dijimos, a que debe existir una discusión durante la realización del examen.

Por supuesto, las Webcams mediante un sistema de procesado de imágenes podrían controlar el uso de documentación o no.

Problemas que se presentan:

- La eliminación del micrófono podría facilitar que personas fuera de la habitación, pero próxima a ella, pudieran colaborar en la resolución del examen.
- Aún con las Webcams, quedarían ángulos muertos en la habitación donde una persona estuviera ayudando a los examinados.
- Una cuestión ajena a la configuración del entorno, y de tipo social, sería la disponibilidad de las personas no discapacitadas que aceptaran desplazarse al lugar del estudiante con problemas de movilidad.

Examen remoto fuera-de-casa individual con y sin documentación

Este entorno presenta todos los retos posibles en la evaluación de un individuo. En este apartado dejamos aquellos entornos relativamente controlables como podía ser la casa del estudiante a otros entornos cambiantes y con una desbordante cantidad de eventos impredecibles y distintos dependiendo del entorno donde se realice.

Este entorno puede darse en ambientes donde el estudiante pueda conectar su ordenador a una red inalámbrica o en recintos donde dispongan de ordenadores para el uso del público, como un cibercafé.

En cualquier caso, la cantidad de gente alrededor de un individuo es impredecible. Los ruidos que puedan aparecer, los móviles cercanos en uso y las posibles interacciones que puedan darse entre el sujeto en cuestión y el resto de personas presentes en el mismo lugar.

El ordenador puede integrar perfectamente la captura de una muestra biométrica a intervalos, pero eso solo asegurará que la persona sentada frente al ordenador sea el individuo correcto. Con una WebCam se podría controlar un cierto barrido del entorno, siempre considerando que todos estos dispositivos estuvieran integrados en el ordenador.

Lo que no se podrá garantizar es el uso propio de un móvil o de otros dispositivos. Mediante unos cascos con micrófonos se podría controlar perfectamente lo que habla, aunque la tarea de filtrar todos los ruidos externos será importante.

El control de documentación se hace tarea imposible, ya que con toda seguridad las Webcams tendrán una gran área donde no llegarán, incluyendo Webcams que tuvieran algún motor de giro.

En nuestro planteamiento inicial, la modalidad remota solo se articula para situaciones con problemas geográficos o de movilidad. En tal caso es más fácil fijar de mutuo acuerdo que sea el recinto habitual, ya sea casa u oficina del estudiante, donde se realice el examen. Sugerir un examen remoto para cualquier individuo como una opción, ajustable a cada estudiante, accesible desde cualquier punto, etc.; en definitiva, un examen a la carta. Tal opción queda lejos de implementarse con la tecnología que en la actualidad se cuenta.

En síntesis, el estado tecnológico actual de desarrollo de Software y Hardware imposibilita los controles de parámetros relevantes de seguridad del examen. Estos parámetros fundamentalmente son: intrusión de audio, falta de control de la imagen y presencia de móvil u ordenadores.

Examen remoto fuera-de-casa en grupo con y sin documentación

Este entorno en la actualidad también se hace difícil de abordar por la cantidad de eventos o acciones que potencialmente pueden ser peligrosas para el resultado final de un examen, como ya comentamos en el punto anterior.

Como siempre, la identificación correrá a cargo de algún dispositivo biométrico integrado en el ordenador. Pero el control del comportamiento de los integrantes del grupo será más complicado. Cada uno puede llevar las Webcams y los micrófonos para estudiar lo que hablan, pero no se podrá controlar la cantidad de modos de comunicación tan cercanos que se pueden desarrollar: papeles escritos, móviles, etc.

Esta configuración hereda todos los problemas de la configuración anterior con el añadido de la falta de control del número de personas integrantes del grupo, sus movimientos y el comportamiento dentro y fuera del grupo.

Conclusión de los entornos de examen planteados

La modalidad de exámenes por ordenador proporciona unos beneficios de logística y coste que hacen de su implantación una idea que cada día cobra mayor fuerza, y constituye una tendencia válida en un futuro inmediato. Se han revisado los posibles entornos para realizar un examen, algunos de ellos se escapan del estudio actual y tan solo se han introducido para ver toda la problemática que se genera en relación a la verificación de la identidad, además del control del comportamiento mayormente en entornos remotos.

Nuestra investigación se centró en este control de identidad en la modalidad de presencial e individual, ya que el paso a exámenes a través de una plataforma educativa ya se está realizando a nivel de contenidos del curso y como encuestas durante el curso. Es decir, una integración de diferentes elementos que hagan posible un examen a través de estos medios es un paso factiblemente realizable.

Los costes en material fungible (fotocopias, papel, tinta, etc.) podrán verse reducidos, aunque el coste de los dispositivos de los diferentes entornos puede resultar, en una primera etapa, bastante caro.

De forma colateral a este conjunto de costes, se debe valorar por parte de la universidad las respuestas a los siguientes interrogantes: ¿hasta dónde llega el límite del control en los exámenes? ¿se invade la privacidad?

ALCANCE DE INTRODUCIR LA TECNOLOGÍA BIOMÉTRICA EN PRUEBAS E-LEARNING

Se realizó un análisis de amenazas para la situación de exámenes presenciales individuales integrados en plataformas educativas (Gil y otros, 2009), para

evaluar según el entorno ya descrito en el apartado anterior, si la biometría puede conducirnos a una solución viable y aplicable en las universidades para los exámenes por ordenador presenciales.

La situación es la siguiente: se introduce la oportunidad de realizar un examen complementario que se evaluará de forma conjunta con la forma tradicional de evaluar. En la forma tradicional los estudiantes asisten al centro y se les entrega un papel con su examen correspondiente, el cual tendrá que rellenar y entregar pasado un tiempo. El examen complementario será un examen tipo Web. Se presentará en el sistema de aprendizaje de Moodle (Martín Galán y Rodríguez Mateos, 2012) y el estudiante podrá visualizarlo en su navegador. Por tanto, el aula donde se realicen los exámenes estará provista de un ordenador por puesto. El ordenador estará conectado al servidor para realizar el examen pero no tendrá acceso a Internet. Una vez que el estudiante realice el examen lo enviará de forma electrónica para su corrección, pero también, imprimirá una copia en papel con sus respuestas de forma que se quede como doble prueba de la realización de un examen.

Con el análisis de amenazas pretendemos ver si hay una justificación razonable para adoptar la tecnología biométrica para controlar estos riesgos (tabla 1). Como nuestro caso se centra en la confiabilidad con que el examen se realiza en cuanto a la identidad del individuo, solo nos centraremos en los que hemos destacado:

- Si el sistema es accesible exteriormente, cualquier experto intruso podría entrar. Si dispone de características de acceso basadas en características físicas del personal encargado será más complicado estos ataques.
- Si hay un gran aforo, el proceso de mirar el carnet de estudiante o tarjeta identificativa ralentizaría todo el proceso, además del error por cansancio humano. Si se dispone de un dispositivo individual por puesto de comprobación de identidad esto se puede ver minimizado.
- Si un examen se realiza por ordenador de forma individual, no se puede monitorizar su identidad. Cualquiera puede saber la contraseña y acceder por otro. Si se dispone de un mecanismo de verificación de identidad se puede comprobar regularmente.

- Cuando el estudiante se da cuenta que va a suspender intentará por todos los medios borrar sus respuestas. Si antes de comenzar un examen ha realizado una comprobación de identidad este dato quedará guardado como prueba de que realizó un examen.

SI	ENTONCES
El módulo de evaluación es defectuoso.	Las respuestas se pueden analizar de forma incorrecta.
El control de acceso no funciona (por ejemplo, botón de “hacia atrás”).	Otros estudiantes pueden ver los resultados del anterior examen.
El sistema es demasiado complejo.	Puede caerse con mayor facilidad.
Un estudiante reclama haber entregado diferentes respuestas de las que se presentan en la muestra impresa.	Existirán problemas de aceptación.
Modificación activa de las respuestas.	Un profesor puede cambiar las respuestas del estudiante después de que el estudiante las responda pero antes de calificar.
Un sistema de evaluación permite acceso desde el exterior.	Un estudiante puede obtener todas las preguntas del examen antes de que se produzca el mismo.
Un estudiante no utiliza el programa como debería durante el examen.	El estudiante puede causar que el sistema termine de forma anormal.
El personal encargado durante el examen realice fallos cruciales durante el tiempo del examen.	Ellos pueden negar haber recibido un examen.
Asistencia de un gran número de estudiantes.	Difícil controlar todas las identidades.
Examen se realiza por ordenador.	Cualquiera puede introducir nombre y contraseña aún no siendo ese usuario.
Un estudiante realiza un mal examen.	Intento de borrar la identidad y las respuestas.

Tabla 1. Especificaciones de riesgos en exámenes Web

Se puede ver que existen unas amenazas de las que debemos hacernos cargo. La identidad del usuario será el papel principal en estas amenazas; conocida su identidad, será imposible que quede inmune ante alguna acción no permitida y malintencionada. También el trasladar los exámenes a la Web trae ventajas e

inconvenientes, la posibilidad de poder monitorizar las acciones de un usuario perfectamente identificado da una nueva baza a la evaluación continua permite ponderarla, lo cual proporciona un entendimiento del aprendizaje del estudiante más extenso. Por supuesto, cualquier medio electrónico podrá ser vulnerable, lo que llevará unas nuevas políticas de seguridad. La biometría aparece como medio para minimizar la probabilidad de las amenazas.

RESULTADOS: EVALUACIÓN POR PARTE DE LOS ESTUDIANTES

Durante el pasado mes de junio de 2010 se pidió, en algunas materias de los laboratorios (Gil, Martín, Díaz, Sancristobal, Castro y Peire, 2008), la participación de los estudiantes con el fin de valorar el uso del control biométrico mediante huella dactilar como método de identificación en pruebas asistidas por ordenador. Los resultados de los cuestionarios cumplimentados por los estudiantes se muestran a continuación.

Características de la muestra

Para analizar los resultados, en primer lugar se destaca las características de la muestra de estudiantes.

El conjunto de estudiantes que realizaron la experiencia de identificación mediante huella durante el proceso de sus prácticas de laboratorio, en total 23 estudiantes, tienen el siguiente perfil: la mayoría está en el segmento de 26 a 35 años de edad, coincidente con el perfil mayoritario de los estudiantes de Ingeniería de la UNED; tienen un título universitario medio, quizás porque el estudiante de la Escuela de Ingeniería Técnica Superior en su mayoría procede de las Escuelas de Ingeniero Técnico; casi en su totalidad son hombres.

Por lo tanto, la muestra está muy próxima al perfil de estudiantes de Ingeniería Industrial de la UNED (ver anuario del IUED curso 2005/6 último publicado IUED, 2005).

Resultados descriptivos

El objetivo de la encuesta (Castro-Gil, Díaz y Gil, 2010; Gil, 2006) se centró en el conocimiento de las actitudes de los estudiantes ante un nuevo medio de control de acceso a las actividades en la formación on-line. A continuación se muestran los resultados descriptivos:

Válidos	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Lo considero muy conveniente	6	26,1	26,1	26,1
Lo considero conveniente	5	21,7	21,7	47,8
Lo considero indiferente	7	30,4	30,4	78,3
Lo considero poco útil	2	8,7	8,7	87,0
Lo considero totalmente innecesario	3	13,0	13,0	100,0
Total	23	100,0	100,0	

Tabla 2. ¿Cómo considera la utilización de registrarse a través de la huella dactilar (control biométrico) en el acceso a los cursos de formación on-line?

Si se descarta la posición ambigua de la indiferencia los estudiantes consideran muy conveniente o conveniente (47,8%) la utilización del registro mediante huella dactilar en el acceso a los cursos de formación on-line. Aquellos que están a favor de utilizar este medio biométrico manifiestan que les parece más seguro, sencillo y rápido que otros medios de acceso. Los que se manifiestan en contra del control mediante huella creen que con la “palabra de paso” es suficiente.

Respecto a la elección del medio biométrico, la tabla 3 decanta a los estudiantes claramente por la huella dactilar (52,2%).

Válidos	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Huella dactilar	12	52,2	52,2	52,2
Control por iris	3	13,0	13,0	65,2
Control facial	1	4,3	4,3	69,6
Control por voz	3	13,0	13,0	82,6
Me resulta indiferente	4	17,4	17,4	100
Total	23	100,0	100,0	

Tabla 3. Si tuviera que elegir un medio biométrico de acceso al curso on-line, ¿cuál elegiría?

En relación a la facilidad de acceso mediante huella con el interface especialmente construido durante el proyecto, los estudiantes piensan que les resulta muy fácil o fácil (78,3%), véase tabla 4.

Válidos	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Muy fácil	9	39,1	39,1	39,1
Fácil	9	39,1	39,1	78,3
Ni fácil ni difícil	4	17,4	17,4	95,7
Difícil	1	4,3	4,3	100,0
Total	23	100,0	100,0	

Tabla 4. Considera que sería fácil la entrada al curso on-line mediante identificación por huella dactilar

Finalmente, nos interesaba saber el nivel de conocimiento y el uso de la biometría. Las tablas 5 y 6 muestran a un estudiante mayoritariamente desconocedor de estas técnicas y que apenas las ha utilizado.

Válidos	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Nivel medio	1	4,3	4,3	4,3
Nivel usuario	8	34,8	34,8	39,1
Nivel sin conocimientos	14	60,9	60,9	100,0
Total	23	100,0	100,0	

Tabla 5. ¿Cómo considera sus conocimientos de biometría?

Válidos	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Lo utilizo a veces	1	4,3	4,3	4,3
Lo utilizo esporádicamente	5	21,7	21,7	26,1
No lo he utilizado nunca	17	73,9	73,9	100,0
Total	23	100,0	100,0	

Tabla 6. ¿Ha utilizado alguna vez el control de acceso biométrico?

En resumen, se ve una tendencia positiva de los estudiantes hacia el uso de la huella dactilar como medio de acceso a la formación on-line porque lo consideran más seguro, sencillo y rápido que otros medios de acceso. Aquellos que manifiestan su oposición al medio consideran que es suficiente con la “palabra de paso”. La huella es el medio biométrico elegido ante varios aunque quizás esta elección viene derivada de ser la más conocida y de mayor penetración en dispositivos de acceso, como por ejemplo, los mismos portátiles. Les ha resultado fácil el acceso con el interface preparado “exprofeso” durante el desarrollo de la presente investigación. Tienen un bajo conocimiento de las técnicas biométricas y la mayoría no las han utilizado nunca.

CONCLUSIONES

Se optó por utilizar una tecnología que identificara a los sujetos inequívocamente, basada en las características físicas o dinámicas de los individuos. Como se vio en el apartado de resultados, los estudiantes en particular preferían el uso de huella dactilar como técnica biométrica por un 52,2% frente a otras técnicas. Ya sea por la aceptación global, por ser la primera técnica biométrica que se desarrolló y por su abaratamiento del mercado, es sin lugar a duda la técnica que más ampliamente se utiliza.

El objetivo central de esta investigación fue discriminar la identidad real de los sujetos que acceden a sistemas de gestión de aprendizaje desde un ordenador que está en el centro de estudios. La justificación es otorgar la calidad y fiabilidad al aprendizaje y a la evaluación del mismo. Mediante la integración del reconocimiento por huella dactilar se consigue cumplir este objetivo, además se extraen las siguientes ventajas y características de nuestra aplicación final:

- Rapidez y sencillez en el registro de nuevos usuarios. Como cualquier plataforma o comunidad se requiere un registro. Cuando se rellenan los datos del formulario con los datos personales y un nombre de usuario y contraseña a elección del usuario se produce también la captura de la huella dactilar. Luego el registro se realiza una sola vez.
- La huella dactilar en la media de edad de estudiantes que usarían la aplicación (de 26 a 35 años) no está muy desgastada por trabajos manuales, así que es una característica universal y única que es válida para la verificación de identidad en nuestro entorno.

- Acceso inmediato mediante la huella, con una verificación 1:1.
- La huella dactilar es encriptada tanto por el software del sensor como por el sistema de gestión de aprendizaje, lo cual hace complicado su manipulación.
- Los datos biométricos se tratan como otro dato más dentro de la base de datos del sistema de gestión de aprendizaje. Nuestra aplicación se integró en Moodle, almacenándose los datos biométricos en la tabla (*mdl_user*) de MySQL (My SQL – lenguaje de consulta estructurado) de Moodle.
- Una contribución al empleo de código libre. Se integró el software de desarrollo de NITGEN (NITGEN, 1998), tecnología del sensor biométrico, al lenguaje PHP (Pre-procesador de Hipertexto) el cual está basado Moodle. NITGEN ofrece diferentes módulos que hacen posible utilizar un abanico grande de lenguajes para diferentes entornos. Dentro de la programación Web, NITGEN trata por defecto ASP (Páginas de Servidor Activo) como lenguaje predeterminado. En esta investigación se trasladó a PHP con Javascript, utilizando archivos HTML para convivir con los archivos base de Moodle. En resumen, se produce una total integración de ambos módulos.
- El administrador del sistema puede gestionar que, una vez finalizado el curso, se produzca el cierre o expiración del derecho a entrar al curso. Esto implicará que los estudiantes que quieran entrar deberán volver a matricularse, lo cual lleva a una continua actualización de la muestra de huella dactilar por parte del sujeto. Esto soluciona cualquier modificación de la muestra ante algún daño o accidente.

Por supuesto, el coste y la privacidad que conlleva tratar datos biométricos de estudiantes pueden suponer un problema para la implantación o extensión del proyecto a ámbitos mayores.

AGRADECIMIENTOS

Los autores quieren agradecer al Ministerio de Ciencia e Innovación Español por el soporte en el proyecto TSI2005-08225-Co7-03 “mosaicLearning: Aprendizaje electrónico móvil, de código abierto, basado en estándares, seguro, contextual, personalizado y colaborativo”; el proyecto TIN2008-06083-Co1 “s-Labs: Integración de servicios abiertos para laboratorios remotos y virtuales distribuidos, reutilizables y seguros”; a la CYTED por el proyecto CYTED-508AC0341 “SOLITE- SOFTWARE LIBRE EN TELEFORMACIÓN”; y agradecer el apoyo del proyecto e-Madrid, S2009/TIC-1650, “Investigación y Desarrollo de tecnologías para el e-learning en la Comunidad de Madrid”.

REFERENCIAS BIBLIOGRÁFICAS

- Castro, M.; Gil, R.; Martín, S.; Colmenar, A.; Díaz, G.; Peire, J. (2006). New Project on Secure Education Services for on-line Learning. *ICEE-2006 International Conference on Engineering Education: Education, Research and Development Fostering Economic Growth*, (155-156).
- Castro-Gil, M.; Díaz, G.; Gil, R. (2010). Fingerprint Identification in LMS and its Empirical Analysis of Engineer Students' Views. En: Blázquez, M.; Castro, M.; Tovar, E.; Auer, M. *IEEE EDUCON 2010 IEEE Engineering Education 2010 - The Future of Global Learning in Engineering Education*. Madrid: Universidad Politécnica de Madrid, (1731-1738).
- Gil, J. A. (2006). *Estadística e informática (SPSS) en la investigación descriptiva e inferencial*. Madrid: UNED.
- Gil, R.; Martín, S.; Díaz, G.; Sancristobal, E.; Castro, M.; Peire, J. (2008). Biometric Identification System in Higher Education Exams: Test in Laboratory Practices. En: Cunningham, P.; Cunningham, M. *Collaboration and the Knowledge Economy: Issues, Applications, Case Studies*, (1549-1556).
- Gil, R.; Martín, S.; Díaz, G.; Sancristobal, E.; Castro, M.; Peire, J.; otros. (2009). On-line and In-room Evaluation Integrated in Learning Management Systems. M-2009. *23rd ICDE World Conference on Open Learning and Distance Education including the 2009 EADTU Annual Conference*. Holanda: EADTU & ICDE.
- Gil, R.; Sancristobal, E.; Martín, S.; Díaz, G.; Colmenar, A.; Peire, J.; otros. (2008). Diseño de Seguridad para Entornos de Evaluación. *INECE'08 II Jornadas Internacionales UPM sobre Innovación Educativa y Convergencia Europea 2008*. Madrid: Universidad Politécnica de Madrid.
- González, J.; Gaudioso, E. (2006). *Sistemas Interactivos de Enseñanza/Aprendizaje*. Madrid: Sanz y Torres, S. L.
- Henríquez Gabante, G.; Ugel Garrido, E. E. (2012). Migración de lo presencial a lo virtual en la asignatura introducción a la computación del programa de enfermería de la UCLA. *RIED. Revista Iberoamericana de Educación a Distancia*, 15 (1), (127-142).

- IUED (2005). *UNED - IUED*. [en línea]. Disponible en: http://portal.uned.es/pls/portal/docs/PAGE/UNED_MAIN/LAUNIVERSIDAD/VICERRECTORADOS/CALIDAD_E_INNOVACION/INNOVACION_DOCENTE/IUED/ANUARIOS/ANUARIOS_UNED_2005-2006.PDF (consulta 2010, 26 de septiembre).
- Martín Galán, B.; Rodríguez Mateos, D. (2012). La evaluación de la formación universitaria semipresencial y en línea en el contexto del EEES mediante el uso de los informes de actividad de la plataforma Moodle. *RIED. Revista Iberoamericana de Educación a Distancia*, 15 (1), (159-178).
- Moodle (1999). *Moodle*. [en línea] Disponible en: <http://moodle.org/> (consulta 2010, 22 de agosto).
- NITGEN (1998). *NITGEN*. [en línea] Disponible en: <http://www.nitgen.com/eng/index.html> (consulta 2010, 8 de agosto).
- Rama, C. (2010). La tendencia a la despresencialización de la educación superior en América Latina. *RIED. Revista Iberoamericana de Educación a Distancia*, 13 (1), (39-72).

PERFIL ACADÉMICO Y PROFESIONAL DE LOS AUTORES

Rosario Gil Ortego. Ingeniera de Telecomunicaciones por la Universidad de Alcalá de Henares y Doctora en Ingeniería Industrial por la ETSI Industriales de la UNED. Obtuvo una beca de formación personal investigador (FPI) por el MCI incorporándose en el DIEEC en 2005. Desde diciembre de 2010 es profesora ayudante en el mismo departamento. Sus líneas de investigación son: seguridad de la información, aplicación y desarrollo de técnicas biométricas en la educación a distancia.

E-mail: rgil@ieec.uned.es

Manuel Castro Gil. Doctor Ingeniero Industrial por la Escuela Técnica Superior de Ingenieros Industriales (ETSII) de la UPM. Actualmente es Catedrático de Universidad del área de Tecnología Electrónica en el DIEEC, ETSII de la UNED. Ha sido Vicerrector de Nuevas Tecnologías de la UNED, así como Director del Centro de Servicios Informáticos de la UNED y Subdirector de Investigación, Subdirector de Gestión Académica de la ETSII de la UNED y Director del Departamento.

E-mail: mcastro@ieec.uned.es

Gabriel Díaz Orueta. Doctor en Ciencias Físicas por la UAM. Ha trabajado durante casi 10 años en *Digital Equipment Corporation*, donde participó en diversos proyectos relacionados con desarrollo de sistemas expertos, así como fue responsable de diversas áreas de formación y consultoría, relacionados con las áreas de comunicaciones y seguridad informática. Desde 2006 trabaja para la UNED y

coordina actualmente el Máster de Investigación de Ingeniería Eléctrica, Electrónica y de Control Industrial.

E-mail: gdiroz@ieec.uned.es

Sergio Martín Gutiérrez. Doctor por el DIEEC de la ETSI de Industriales de la UNED en 2010. Es Ingeniero Superior de Informática, Especialidad Aplicaciones y Sistemas Distribuidos, por la UC3M. Ingeniero Técnica de Informática, Especialidad Sistemas por la UPM. Ha participado en proyectos de investigación, relacionados con movilidad e inteligencia ambiental, localización y redes inalámbricas, así como en proyectos relacionados con “e-learning”, laboratorios remotos y virtuales y nuevas tecnologías aplicadas a la enseñanza.

E-mail: smartin@ieec.uned.es

Elio San Cristobal Ruiz. Doctor en sistemas de ingeniera Eléctrica, Electrónica y de Control por la ETSI de Industriales de la UNED. También posee los títulos de Ingeniero Informático, especialidad en Ingeniería del Software, por la Universidad Pontificia de Salamanca (UPS) e Ingeniero Técnico en Informática de Sistemas por la misma Universidad. Actualmente está trabajando para el Centro de Servicios Informáticos de la UNED.

E-mail: elio@ieec.uned.es

DIRECCIÓN DE LOS AUTORES

Departamento de Ingeniería Eléctrica,
Electrónica y de Control (DIEEC)
Escuela Técnica Superior de Ingeniería
Industrial
UNED
C/ Juan del Rosal, 12
Ciudad Universitaria, Madrid, 28040

Fecha de recepción del artículo: 13/09/11

Fecha de aceptación del artículo: 25/01/12

Como citar este artículo:

Gil Ortego, R.; Castro Gil, M.; Díaz Orueta, G.; Martín Gutiérrez, S.; San Cristóbal Ruiz, E. (2012). Nuevo modelo de evaluación asistida por ordenador en educación a distancia. *RIED. Revista Iberoamericana de Educación a Distancia*, volumen 15, nº 2, pp. 143-170.