

Reflexiones sobre la Gestión de Riesgos en la Evaluación Telemática dentro del contexto de la E.T.S.I de la Universidad de Sevilla

Departamento de Ingeniería Telemática¹
E.T.S. Ingeniería
Universidad de Sevilla

1. INTRODUCCIÓN Y OBJETIVOS

La evaluación telemática supone riesgos que el profesor debe saber gestionar con las oportunas contramedidas. La implementación de contramedidas supone necesariamente un coste en tiempo o recursos, por lo que debe buscarse el equilibrio en esa relación entre coste y beneficio. El objetivo de este trabajo es ofrecer al profesor, especialmente de ingeniería, una reflexión sobre los riesgos inherentes a la evaluación telemática y sugerir algunas soluciones que lo ayuden a tomar una decisión bien fundada para su asignatura.

Los objetivos concretos del presente trabajo se centran en:

- Proporcionar información sobre los riesgos de la evaluación telemática
- Revisar las alternativas existentes para modificar la situación de riesgo
- Proponer tipologías de evaluación telemática con diferentes niveles de riesgo
- Compartir la experiencia acumulada hasta el momento en la evaluación telemática

En todo caso, las contramedidas aplicables dependerán de factores intrínsecos a la asignatura (naturaleza, objetivos de su evaluación), del profesor (competencia en el manejo de la tecnología, aversión al riesgo) y de la organización docente (número de alumnos por asignatura) y se verán condicionadas por los recursos tecnológicos y humanos.

Aunque el alcance estas notas que pretende orientar a los profesores de la Escuela Técnica Superior de Ingeniería de esta Universidad se limita a la plataforma de docencia telemática *BlackBoard* existente en la Universidad de Sevilla (ev.us.es), sus aportaciones son en gran parte aplicables a otros ámbitos y plataformas de docencia universitaria.

2. CONTEXTO: RIESGOS EN LA EVALUACIÓN TELEMÁTICA

La evaluación telemática no es sino la valoración por medios telemáticos, cuando es posible, de las competencias, destrezas y habilidades adquiridas por los alumnos. Por tanto es tan variada como la evaluación tradicional y puede articularse mediante actividades de distinto tipo:

1. Exámenes individuales
2. Realización de trabajos y proyectos individuales o en grupo
3. Participación en actividades y seminarios

Esas actividades pueden efectuarse de forma síncrona (todos los alumnos a la vez) o asíncrona (cada alumno a su ritmo). Según la temporización de esas actividades, la evaluación puede ser continua o basada en examen final.

La ilustración 1 refleja de forma genérica un escenario de exámenes telemáticos con algunos elementos de riesgo potencial:

¹ Corresponding authors: Rafael Estepa (rafaestepa@us.es), Juan M. Vozmediano (jvt@trajano.us.es) y Antonio Estepa (aestepa@us.es)

² si suponemos un comportamiento homogéneo de los alumnos, la fórmula se reduce a: $R = A \times P \times I$.

³ En la ETSI se utiliza adicionalmente una herramienta que permite exámenes con preguntas parametrizadas y respuestas tipo test que se corrigen de forma automática. Esto podría asimilarse a un examen E.4

⁴ Aunque la combinación de máquinas virtuales y túneles o escritorios remotos puede hacer creer que el alumno

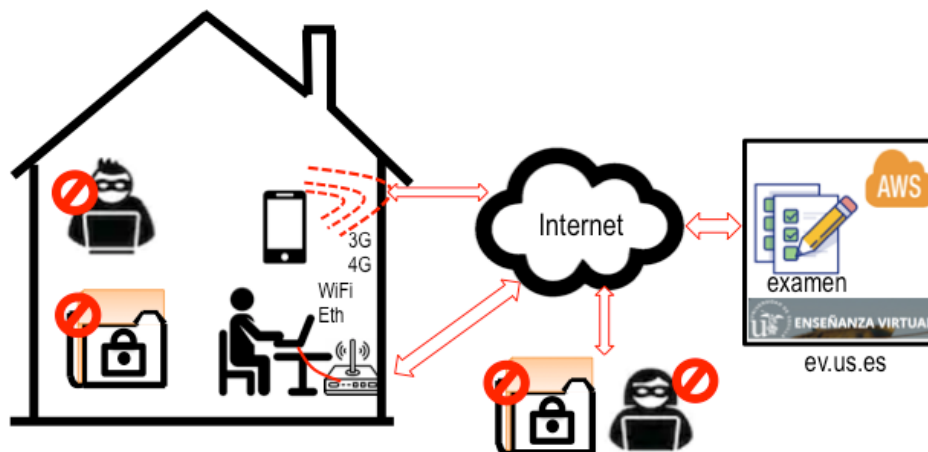


Ilustración 1. Escenario en la realización telemática de exámenes

Se parte de que el alumno dispone en su domicilio de un PC o tablet con cámara con el que accederá a la plataforma (ev.us.es) utilizando Internet. Dicho acceso puede ser muy variado: fibra, ADSL y acceso móvil 4G/3G. Sin embargo, durante la realización del examen cada alumno podría contar con la asistencia, no autorizada, de material o de terceros.

De forma general, el nivel de riesgo, R, se puede definir como el producto de la probabilidad de que se materialice una amenaza/contratiempo/desgracia por las consecuencias que tiene dicha materialización, es decir $R = P \times I$, donde P es la probabilidad de materialización de la amenaza (incidencia en un examen, copiar, etc...), e I es el impacto en el examen en caso de materializarse. La gestión del riesgo abarca tanto una estimación del mismo, como la adopción de contramedidas que permitan mitigarlo hasta un nivel aceptable para el profesor. A continuación se analizarán los riesgos en el escenario anterior y se propondrán contramedidas que permitan mitigarlo.

En este escenario podemos distinguir dos tipos de riesgo:

1) Riesgo técnico: El riesgo técnico es el que compromete la ejecución del acto de evaluación. El equivalente tradicional sería un corte de luz o la indisponibilidad del aula de examen. Los síntomas son la pérdida de interactividad o falta de respuesta en el navegador, la denegación de acceso a la plataforma y en último caso la expulsión de los usuarios de la misma. Las causas pueden ser:

- a) problemas de indisponibilidad del servicio de ev.us.es: Los problemas en la disponibilidad del servicio afectan a todos los usuarios. Es posible identificar las siguientes amenazas o contratiempos:
 - **IS1:** congestión en el servidor por exceso de carga.
 - **IS2:** el servidor está indisponible por actualización o por otros motivos técnicos
 - **IS3:** fallo en las comunicaciones con la plataforma imputable a la Universidad, con los servidores locales o en la nube.
- b) problemas en el acceso a ev.us.es: Los problemas en el acceso afectan sólo a algunos alumnos, y pueden deberse a fallos en sus equipos o en su infraestructura de acceso a Internet. Podemos identificar las siguientes amenazas o contratiempos:
 - **IN1:** Acceso con capacidad insuficiente.
 - **IN2:** Corte de comunicaciones. Puede deberse a fallos en el operador de red o a la caída del suministro eléctrico.
 - **IN3:** Fallo en los equipos del alumno hasta la conexión con el operador (hardware o software del terminal o problemas con la WiFi).

2) Riesgo confiabilidad: El riesgo de confiabilidad compromete la validez de la evaluación por falta de probidad no detectada en el cumplimiento de las normas de la misma. Una evaluación en la que no pueden controlarse las condiciones no mide lo que debería medir y el proceso mismo queda desvirtuado. Si interpretamos la falta de probidad en un examen (la tradicional 'copia') como una amenaza, los principales vectores de actuación que podemos identificar serían:

V1. Acceso a material no autorizado. El alumno es el único autor del ejercicio pero utiliza material que no se corresponde con las condiciones para las que aquel fue diseñado. El equivalente tradicional sería las chuletas.

V2. Colaboración con terceros: El alumno no es el único autor del ejercicio, ya que cuenta con la asistencia de terceros (compañeros o expertos) que lo suplantan en todo o en parte del mismo. El equivalente tradicional es la copia de compañeros o amigos dentro o fuera del aula. La suplantación de la identidad del alumno por otra persona es otro caso particular de este vector de actuación.

V3. Simulación de incidente: El alumno, a la vista de su desempeño ante el ejercicio, simula un incidente técnico para conseguir alguna ventaja (contar con más tiempo, sortear la vigilancia o repetir el ejercicio en otro momento).

Resulta evidente que la evaluación telemática exagera estas amenazas ya que por un lado dificulta la vigilancia del profesor y por otra facilita el acceso a información (tanto por medios tradicionales como telemáticos) y la comunicación con terceros.

La materialización de cualquiera de estos dos riesgos traería como consecuencia un fracaso en la realización del examen, por lo que deben tomarse las medidas para reducir dichos riesgos.

3. GESTIÓN DEL RIESGO TÉCNICO

3.1 Análisis del riesgo

El efecto de un incidente en el riesgo asociado al desarrollo de un examen dependerá básicamente de la duración del examen y del tiempo de indisponibilidad del examen para el alumno. Por norma general, el alumno es muy sensible a cualquier incidente que le reste tiempo de examen, por lo que el impacto para éste será alto. Si el problema afecta a todos los alumnos el impacto será mucho mayor, y aún más grave si el incidente impide que el alumno entregue el examen. En la siguiente tabla se refleja una estimación del riesgo asociado con cada amenaza/contratiempo identificado.

	Riesgo			Observaciones
	P (0-5)	I (0-5)	R=P x I (0-25)	
IS1	0.5	3-5	1-5 – 2.5	<i>Blackboard</i> está en Amazon. Si se cae, coincidirá con el fin de la civilización occidental. No obstante, existe una pequeña posibilidad de saturar los recursos <i>contratados o disponibles</i> para el servidor en momentos muy puntuales (también es posible bloquear las peticiones por confusión con un ataque de negación de servicio contra el servidor).
IS2	0.5	5	2.5	Los mantenimientos son avisados con antelación. Por el historial, entendemos que es poco probable un fallo en el software servidor.
IS3	1	3	3	Los sistemas están bien dimensionados y gestionados, pero los fallos de equipos o de proveedores de acceso son posibles y, aunque se arreglen con rapidez puede afectar al examen
IN1	1-3	1-2	1-6	El caudal contra Internet necesario para según qué tipo de examen no es mucho, pero el acceso a Internet en ciertas zonas geográficas es mediocre o malo, por lo que los fallos pueden venir más probablemente por el acceso <i>Wifi</i> del dispositivo al punto de acceso/router (P=2). Estos fallos suelen ser intermitentes (errores puntuales), no afectando a todo el tiempo de examen.
IN2	1	3	3	Una caída de comunicaciones por problemas del operador o de la compañía eléctrica es muy improbable. De ocurrir se produce en momentos puntuales por picos de tráfico y no suelen prolongarse mucho, pero según el momento en que ocurra puede afectar gravemente al examen.
IN3	1	2	2	Los equipos no suelen averiarse y los posibles problemas de software se

3.2 Mitigación del Riesgo

Para reducir los niveles de riesgo anteriores, podemos identificar las siguientes contramedidas que actuarán, generalmente, disminuyendo la probabilidad de ocurrencia (P):

- **Ajuste Red Local:** Reducir el caudal de datos contra Internet, eliminando otras fuentes que consuman datos durante el examen (en especial videos, música, etc...). Tras restringir el resto de las fuentes que envían o reciben datos sobre la red de acceso es recomendable realizar un test de velocidad de acceso a Internet. (por ejemplo: www.test-velocidad.com). También se debe recomendar al alumno realizar el examen (preferentemente) desde un PC/portátil conectado por Ethernet (cable) a su *router* de operador (el cable puede medir hasta 90 metros). Si no es factible, ubicarse lo más cerca posible del punto de acceso *wifi*. Acción a ejecutar por el alumno. Disminuye el riesgo de problemas en la red de acceso.
- **Verificación Previa:** Realizar un ensayo previo al examen para que así el alumno pueda entender y aceptar las condiciones del examen, así como detectar de forma precoz cualquiera de las amenazas/contratiempos identificados de forma que puedan corregirse. Para ello se puede hacer un test de prueba donde respondan a alguna pregunta evidente (su nombre, o que han realizado el test sin incidencias) o que aporten información de utilidad (registro en smowl, una imagen con un test de velocidad de acceso a Internet, su dirección IP, tipo de dispositivos, etc...). Permite al alumno y al profesor detectar posibles problemas con tiempo para resolverlos. Acción a ejecutar por alumno y profesor. Disminuye el riesgo de todas las amenazas anteriores.
- **Equipo y Red Respaldo:** Tener un dispositivo alternativo (Tablet, por ejemplo) preparado y configurado para realizar el examen si el dispositivo principal falla. Acción a ejecutar por el alumno. Disminuye el riesgo de la amenaza IN1. Tener un dispositivo móvil 3G/4G alternativo a la conexión de Internet principal (mejor si es con otro operador distinto), preparado y configurado para compartir su conexión a Internet, si la conexión principal falla. Acción a ejecutar por el alumno. Disminuye el riesgo de la amenaza IN3
- **Reducción de Carga:** Repartir a los alumnos en varias tandas de acceso al examen para evitar la coincidencia puntual del comienzo del examen. Se puede realizar de varias formas: anunciar distintas horas de inicio (p.e. a las 10:00 los que su primer apellido comienza por A-G y a las 10:01 el resto) o dividir a los alumnos en dos o más grupos y asignar el examen a cada grupo con horas de comienzo distintas. Alternativamente se deben reducir el tamaño de las imágenes utilizadas en el examen y prescindir de elementos multimedia para reducir el tiempo de descarga. Acción a ejecutar por el profesor para pruebas muy masivas. Disminuye el riesgo de la amenaza IS1
- **Conexión de Control del Profesor:** Consiste en tener un canal abierto con los alumnos donde ellos puedan comunicar las incidencias e intentar resolverlas. Se puede utilizar un chat o cualquier medio similar (*Collaborate chat*, foro, incluso email). Acción a ejecutar por el profesor y el alumno. Disminuye el riesgo de la amenazas que afectan a servidores.

3.3 Recomendaciones

Entendemos que el profesor debería, como mínimo, tomar las siguientes contramedidas.

- Informar al alumno para que realice: **Ajuste Red Local** y **Equipo y Red Respaldo**
- Se recomiendan las contramedidas **Conexión de Control del Profesor** (resulta de utilidad para detección precoz de incidencias) y **Verificación Previa** (aprovechar el chequeo para informar al alumno de las condiciones del próximo examen -tipo de examen, medidas de control, etc...- y recabar la aceptación de las mismas e información de utilidad)

En el caso de exámenes muy masivos, implementar **Reducción de Carga**.

Cuando las incidencias son masivas suele ser problema del servidor (IS1,IS2,IS3) y no hay otra medida que reprogramar el examen (si el impacto ha sido grande) o tomar medidas correctivas generales sobre las condiciones de la prueba realizada (reducir la penalización de los fallos, modificar el peso de los distintos apartados...) para incidencias menos graves. Cuando las incidencias son individuales y están debidamente justificadas se puede optar

por reprogramar el examen a los alumnos implicados (no necesariamente el mismo tipo de examen), o por corregir el examen con las preguntas respondidas hasta el momento de la incidencia (si el impacto ha sido pequeño).

4. GESTIÓN DEL RIESGO DE CONFIABILIDAD

Durante el examen el alumno podría incumplir las condiciones de realización establecidas (de las que se ha informado convenientemente al alumno) buscando ventajas inapropiadas. Esta falta, conocida como falta de probidad, es un fraude duramente castigado en el Reglamento de Disciplina Académica. En los exámenes telemáticos, donde es imposible la supervisión directa del profesor, este riesgo se dispara, por lo que resulta crítica su gestión.

4.1 Análisis del riesgo

De forma general, el riesgo de fraude, R, en un examen con un número de alumnos A, podría definirse como:

$$R = \sum_{i=1}^A P_i \times I_i$$

Donde P_i es la probabilidad de que el alumno i tenga una ventaja indebida no detectada, e I_i sería el impacto en el fraude que produce dicha ayuda². Los elementos que influyen en cada uno de los factores anteriores son:

- Probabilidad de ocurrencia: $P_i = D_{ay} \times O_{ay} \times H_{ay}$

Donde D_{ay} es la disponibilidad de la ayuda (en ella influyen el tiempo de acceso a la ayuda y la posibilidad de encontrarla –proporcional al número de alumnos y dificultad de encontrar expertos en asignatura-), O_{ay} es la capacidad de encubrir la ayuda ilegítima (es decir, que no sea detectada por el profesor) y H_{ay} es el efecto llamada dependiente del éxito consolidado de la amenaza en ocasiones anteriores por el conjunto de alumnos

- Impacto: $I_i = C_{ay} \times F_i$

Donde C_{ay} se corresponde con el incremento de calificación que supone la ventaja obtenida y F_i es el peso o fracción de la nota final que tiene el examen en la asignatura.

Podemos, por tanto, concluir que el riesgo sigue la siguiente ecuación:

$$R = \sum_{i=1}^A D_{ay} \times O_{ay} \times H_{ay} \times C_{ay} \times F_i$$

Cada tipo de examen tendrá un riesgo base asociado distinto. Los tipos de exámenes que entendemos de mayor utilidad en la ingeniería se reflejan en la siguiente tabla:

<p>Examen escrito basado en preguntas de respuesta corta. Las preguntas de respuesta corta se responden sin adjuntar el razonamiento o cálculo que justifica la respuesta. En función del número de preguntas disponibles y de su presentación tenemos</p>	<p>E1: el mismo test para todos los alumnos Las preguntas son iguales, en el mismo orden y las respuestas son iguales y en el mismo orden para todos los alumnos</p>
	<p>E2: las mismas preguntas. Las preguntas y repuestas son iguales para todos los alumnos, pero puede variar el orden en que se presentan ambas</p>
	<p>E3: un porcentaje de preguntas (tasa de reutilización) serán iguales Las N_e preguntas de cada uno de los A exámenes se obtienen muestreando o parametrizando un banco de N_i preguntas, con $N_i < A * N_e$.</p>
	<p>E4: distinto test para todos los alumnos Cada alumno tendrá un juego de preguntas distinto. Esto puede conseguirse mediante la realización de un banco con $N_e * A$ preguntas diferentes (válido para</p>

² si suponemos un comportamiento homogéneo de los alumnos, la fórmula se reduce a: $R = A \times P \times I$.

	pocos alumnos) o por la parametrización de las preguntas.
Examen escrito de desarrollo. La respuesta debe acompañarse de los cálculos y desarrollos que la justifican. Es el método más fiable para evaluar el conocimiento de la materia	E5. Desarrollo del examen completo (p.e. 2 o 3 h de examen) El alumno recibe el enunciado del examen y dispone de un tiempo para realizarlo bien en el ordenador bien en papel, tras lo cual debe enviarlo directamente o entregarlo escaneado/fotografiado al profesor. <ul style="list-style-type: none"> • E5.1: examen con los mismos apartados para todos • E5.2: examen con los mismos apartados pero parametrizados (p.e. fecha nacimiento, dni) • E5.3: un porcentaje de apartados serán iguales para todos los alumnos • E5.4: distintos apartados para todos los alumnos
Exámenes orales en directo	E6. Defensa de su trabajo o conocimiento individual en directo El examen puede ser grabado (informando al alumno) para preservar evidencias del mismo.
Trabajo escrito	E7. Trabajos a realizar por el alumno de forma asíncrona (plazo largo) Este tipo de actividad no presenta novedades ya que es de naturaleza no presencial si bien no es viable realizarlo para cada alumno si son muchos.

Tabla 2. Tipologías de examen

Obviamente, la carga de trabajo para el profesor difiere en cada uno de los tipos de examen, y para cada tipo de asignatura. Las asignaturas de primeros cursos son especialmente críticas pues el elevado número de alumnos implica un coste desmedido en la carga de trabajo del profesor para algunos tipos de exámenes. Entendemos que en la plataforma ev.us.es es posible realizar todos los tipos de examen señalados en la tabla anterior³.

Los exámenes telemáticos orales son, quizá, los únicos que permiten preguntas de memorización sobre contenidos impartidos. Los test tienen la ventaja de la corrección automática y el inconveniente del tiempo de generación de las preguntas. En función de la materia del examen es posible automatizar la realización de problemas individuales para cada alumno (E4, E5.4) utilizando herramientas de sustitución de variables en el texto con valores distintos por alumno que indique cómo deben ser las sustituciones para forzar distintos problemas o distintos datos para un problema (ver Anexo I).

Los diferentes tipos de exámenes influyen en la efectividad de los distintos vectores de fraude (V1, V2 y V3). En la siguiente tabla se muestra para cada tipo de examen una estimación del riesgo,:

Tipo de Examen		Riesgo (1-5)	Observaciones
Respuesta Corta	E1	5	Muy insegura
	E2	4.5	Ligera reducción en vectores V2
	E3	4-3	Reducción en V2 inversamente proporcional a la tasa de reutilización
	E4	2	Reducción fuerte en vectores V2
Desarrollo	E5.1	5	Muy insegura
	E5.2	3	Reducción en vectores V2
	E5.3	3.5	Reducción en V2 inversamente proporcional a la tasa de reutilización
	E5.4	2	Reduce fuerte en vectores V2
Oral	E6	1	Reducción fuerte en todos los vectores: V1, V2 y V3
Trabajos	E7	5	Muy insegura

Tabla 3. Riesgo base según tipo de examen

4.2 Mitigación del riesgo

La eliminación total del riesgo, cualquiera que sea el tipo de examen, es imposible, dada la abrumadora variedad de alternativas para implementar las amenazas. Las soluciones milagrosas aparecidas en los medios de comunicación, algunas de las cuales no pueden por menos que verse con cierta ternura por lo inocente de su planteamiento

³ En la ETSI se utiliza adicionalmente una herramienta que permite exámenes con preguntas parametrizadas y respuestas tipo test que se corrigen de forma automática. Esto podría asimilarse a un examen E.4

cuando no por su insolvencia técnica o práctica, suelen enfocarse bien en alumnos que sean *analfabetos tecnológicos*, bien en amenazas individuales. Lamentablemente en nuestro entorno el alumno puede ser más experto que el profesor y las amenazas pueden materializarse simultáneamente. Las Universidades a distancia son conscientes de este hecho y por ese motivo realizan exámenes presenciales adicionales a los telemáticos.

Las siguientes variables de control pueden ser utilizados como contramedidas para reducir el riesgo, aunque algunas de las contramedidas también pueden ser neutralizadas:

- **Password:** Comprobación de la identidad en el acceso al contenido del examen. (aunque el alumno puede suministrar las credenciales identificativas a otros). Puede aplicarse en el control de acceso al recurso telemático (examen) o cifrando el examen (winzip lo permite) y distribuyendo a los alumnos una clave de descifrado al comienzo del mismo.
- **Smowl:** Control de presencia automatizado ante la cámara -gestión parcial de identidad- y de la dirección IP utilizada⁴. Necesitaría aceptación por parte del alumno y disponer de una cámara. Esta medida, aunque tan sólo consigue detectar parcialmente los vectores de ataque V2 (cuando la ayuda es presencial), tiene también un carácter disuasorio sobre el vector de actuación V1
- **Tiempo:** Tiempo de realización del examen: $T = T_h$ (tiempo holgado) o T_a (tiempo ajustado). Aplicar un Tiempo ajustado⁵ (T_a) disminuye el riesgo para todos los vectores de ataque V1 y V2. Cuidado, también influye en el impacto en caso de un problema técnico.
- **Concurrencia:** Concurrencia (todos los alumnos a la vez). Misma hora de comienzo y fin para todos.
- **NoBack:** Preguntas mostradas de una en una y sin vuelta atrás.
- **SingleNoSummary:** No mostrar la realimentación final con todas las preguntas resueltas. Se dará la realimentación al finalizar el tiempo de examen (basta ir grabando el examen mientras se realiza).**SA:** (*SafeAssign*).
- **SafeAssign:** Comprobación antiplagio integrada en ev.es.es que permite detectar si dos trabajos / actividades presentados comparten el mismo contenido. Busca en fuentes externas (Internet) y en los trabajos presentados por otros compañeros. El documento entregado por el alumno debe ser de tipo texto (Word, pdf, ...). Aplicable a contenidos tipo: Actividad en Blackboard.
- **Audio/Video:** Activación del audio/vídeo durante el examen (*Collaborate*). Exige que el alumno disponga de cámara. Necesitaría la aceptación por parte del alumno. Aplicar **Audio/Video** para facilitar detectar los vectores de actuación V1. Este control es solo aplicable con pocos alumnos. También reduce posibilidad (en menor proporción) de vectores de actuación V2 al poder observar el uso de dispositivos alternativos
- **Random Query:** Elegir preguntas aleatoriamente de un banco de preguntas
- **Random Answer:** Barajar las respuestas antes de presentarlas
- **Evidencias Incidentes:** El alumno debería ofrecer evidencias (por ejemplo un test de velocidad de acceso a Internet) y el profesor recopilar evidencias del comportamiento del alumno (*logs o informes* de enseñanza virtual).
- **Restringir Ubicación:** Permite dar acceso al examen sólo a los equipos que provienen de una determinada dirección IP. Si se dispone de la dirección IP utilizada por el alumno desde su domicilio permitiría aplicar esta restricción para evitar que desde otra dirección IP, pero conociendo su uvus, alguien pudiera, en remoto, suplantar la identidad del alumno. No obstante podría hacerlo accediendo por escritorio remoto a su ordenador o si directamente si está en la misma ubicación. Esta medida es complicada de implementar y necesitaría de un canal de control del profesor para actualizar la lista de IPs permitidas antes posibles cambios de dirección (por reseteo del router, por ejemplo)

En *Blackboard* se pueden utilizar todas estas contramedidas directamente⁶, y la mayoría también están disponible en otro tipo de plataformas de enseñanza muy difundidas (*Moodle*). El alta de los alumnos y la medida PS de acceso (uvus) están por defecto activas en *Blackboard*. Obviamente, no todas las contramedidas tienen sentido en todos los tipos de examen.

⁴ Aunque la combinación de máquinas virtuales y túneles o escritorios remotos puede hacer creer que el alumno está en cualquier sitio aunque la cámara esté en uno y el equipo en otro

⁵ También es posible, a fin de ajustar el tiempo, utilizar modalidades de calificación dependiente del mismo, **PDT**, donde la calificación tiene en cuenta el tiempo empleado en hallar la respuesta, primando la velocidad

⁶ Existen otras contramedidas no contempladas en este trabajo (ver apartado: Limitaciones del trabajo).

Las contramedidas aplicadas en cada caso tendrán el efecto de disminuir el riesgo hasta un valor residual. Recordemos la ecuación del riesgo de fraude. $R = \sum_{i=1}^A D_{ay} \times O_{ay} \times H_{ay} \times C_{ay} \times F_i$. Veamos cómo reducir los distintos factores del riesgo introduciendo distintos controles con las contramedidas anteriormente descritas:

- Reducción de la disponibilidad de ayuda (D_{ay}):
 - Contramedidas par disminuir el tiempo de acceso a la ayuda: **Tiempo** ajustado (T_a) y **Password**.
 - Contramedidas para disminuir la posibilidad de conseguirla: **Tiempo** ajustado (T_a), **Concurrencia**, **Random Query y Random Answer**, **NoBack**, **SingleNoSummary**, **Restringir Ubicación**.
- Reducción de la capacidad de detectar el fraude (O_{ay}) y el efecto llamada (H_{ay}): imponer controles de detección⁸ también persuade a los alumnos de buscar ayuda. Los controles aplicables serán.
 - Contramedidas: **Smowl**, **Audio/Video**, **SafeAssing**, **Evidencias Incidente**
- Reducción de incremento en la calificación por la ayuda obtenida (C_{ay}). Resulta complicado actuar sobre este factor, se podría incrementar el número de preguntas y su variabilidad.
- Reducción de la fracción del examen en la nota final (F_i): Obliga a la realización de varias pruebas (de distinta tipología si pudiera ser a fin de reducir las debilidades de una tipología concreta) para superar la asignatura⁹. Permite también correlar en el tiempo los resultados y detectar posibles fraudes. Por el contrario, representa una mayor carga de trabajo.

En el Anexo I del presente documento es posible encontrar una descripción más detallada sobre cómo implementar los distintos tipos de exámenes y contramedidas en la plataforma *BlackBoard*.

4.3 Recomendaciones

De forma general, cuando mayor riesgo base tiene un tipo de examen, necesitaremos más contramedidas para mitigarlo. La selección de contramedidas dependerá, en general, del nivel de riesgo aceptable para el profesor-influenciado por su percepción del riesgo- y del número de alumnos.

A modo de orientación para los casos más utilizados en la ETSI, proponemos las siguientes recomendaciones¹⁰. La pertinencia de estas recomendaciones dependerá del tipo de examen a realizar

- Preguntas de problemas (desarrollo): Aplicar siempre controles **Tiempo y Concurrencia**
 - Forma de presentar el examen:
 - Si es el mismo enunciado para todos: (parametrizado –examen E5.2- o no –E5.1-), se puede adjuntar un documento (PDF¹¹, TXT, HTML o imagen) en un contenido tipo examen con *Blackboard*
 - Requiere vigilancia alta (posibles controles adicionales: *Smowl*, Audio/Video)
 - Si hay distintos enunciados debemos distribuirlos para cada alumno o grupos de alumnos (ver final del Anexo I, sobre cómo generar exámenes personalizados)
 - Si hay pocos grupos se pueden realizar varios exámenes (uno por grupo) y asignarlos a cada grupo en *Blackboard*, aplicándose para cada grupo las recomendaciones del caso “Mismo enunciado”. Alternativamente se puede enviar el examen por correo a cada alumnos.
 - Si hay un examen individual por cada alumno lo mejor es mandarlos por correo electrónico. En tal caso hay que dar un margen de tiempo a la recepción, verificar que ha llegado el correo y solución de contingencias. Para asegurar la concurrencia

⁸ Nótese que estos controles deben generar evidencias que deben ser custodiadas (informar al alumno/aceptar cesión de datos con un fin determinado). La obtención de esas evidencias debe contar con el respaldo normativo adecuado.

⁹ En caso de contratar a un profesor externo como ayuda le costará más caro el servicio.

¹⁰ Aviso: estas recomendaciones pueden considerarse una estrategia para afrontar los riesgos de la evaluación telemática. Nadie publica su estrategia con antelación. Dicho de otro modo, no es deseable que esta información se distribuya al alumnado.

¹¹ PDF es un tipo de fichero que contiene un documentos formateado para ser impreso. Es fijo, se muestra siempre igual independientemente del soporte, por lo que no es un cómodo de visualizar en pantalla (sobre todo en pantallas reducidas de móviles - compruebe cómo los periódicos digitales no lo usan) y su uso en la web solo se justifica si la alternativa es aún peor (distribuir ficheros .doc de Word).

- se puede que enviar el examen cifrado y al comienzo del mismo se da la clave para que todos tengan el examen a la vez (con Zip o Arj)
- Forma de recoger las respuestas: crear el examen con preguntas tipo: *respuesta de archivo*.
 - Si se puede, que la respuesta del alumno sea en papel. Ventajas: requiere menos tiempo al alumno y tenemos su caligrafía (posible chequeo posterior). Inconveniente: necesita digitalización del examen –más tiempo/incidencias- (si hacen foto con el móvil, tener en cuenta que cada foto es un fichero, por lo que tendría que hacerse tantas preguntas tipo: *respuesta de archivo* como folios posibles se puedan entregar).
 - Para evitar la digitalización usar un editor de texto externo (p.e. Word), y que el fichero lo entreguen en formato pdf
 - Adicionalmente, se puede indicar al alumno que envíe el examen por correo electrónico al profesor.
 - Control del progreso: es posible repartir los diversos ejercicios (o apartados del examen) en distintas preguntas de un contenido tipo examen, a las que el alumno debe ir respondiendo (controles aplicables: **NoBack, SingleNoSummary**).
 - También se puede hacer un examen diferente por cada pregunta para controlar el tiempo de entrega de cada una individualmente. El profesor activa las preguntas cuando llegue su momento.
 - Preguntas de contenido teórico: Aplicar siempre controles **Tiempo y Concurrencia**
 - Exámenes orales (examen tipo E6): Se pueden emplear para pocos alumnos con unos 20 minutos por alumno. Se puede examinar en paralelo con varios profesores y/o varias sesiones de examen en horario de clases o de examen programado para no solapar con otras asignaturas. En la ETSI no estamos habituados a este tipo de examen, salvo para las defensas de trabajos, así que conviene recordar que, si las preguntas no son triviales, el alumno debe contar con unos minutos iniciales para reflexionar, ordenar ideas y articular la respuesta.
 - Exámenes tipo test/cuestiones (hay muchas posibilidades: respuesta múltiple, verdadero/falso, etc...): asumir que tendrán libros y apuntes delante, así como posibilidad de comunicarse con terceros.
 - Si son las mismas para todos (examen tipo E2). Aplicar al menos las siguientes contramedidas **Random Query y Random Answer, NoBack, SingleNoSummary**
 - Posible vigilancia adicional: **audio/video, smowl**
 - Sin hay probabilidad de que sean las preguntas sean distintas (examen tipo E3), aplicar **Random Query, Random Answer y SingleNoSummary**. Si la tasa de reuso es baja (banco de preguntas muy grande) se puede dar algo más de tiempo y que tengan vuelta atrás, sabiendo que en este caso las preguntas quedarán “quemadas” tras su uso
 - Posible vigilancia: smowl o nada.
 - Suplantación de identidad: Excepto en exámenes orales, es imposible verificar la identidad. Se puede mitigar el riesgo con una validación con audio/video al comienzo (ver cara y dni) o aleatoriamente durante el examen. Otras medidas como **Smowl** son menos efectivas pero aplicables a mayor escala. En exámenes escritos digitalizados se podría validar la letra del alumno frente a una referencia obtenida de forma fiable (video o manuscrito con firma en la aceptación de las condiciones del examen) o cotejarla con exámenes del mismo alumno en otras asignatura. Por último, podemos verificar las direcciones IP de todos los alumnos y cruzarlas después para detectar cambios (tener en cuenta que las direcciones IP no son fijas, el proveedor puede cambiarlas, no debe haber dos exámenes resueltos vinculados a la misma IP)
 - Información de las condiciones de examen y aceptación de las mismas: Recabar dicha información con anterioridad al examen por los mismos medios que se vayan a utilizar en el examen (se aprovecha para acostumbrar al alumno a la dinámica y corregir problemas). Las condiciones deben tener soporte jurídico, y la no aceptación de las mismas podría suponer una reprogramación del examen para dicho alumno con otra tipología -por ejemplo examen oral (pues no es de esperar un gran número de casos) o, en caso extremo, podría suponer que la asignatura cambiara de categoría en la adenda por COVID-19.
 - Incidencias durante el examen: Realizar chequeo previo e informar a los alumnos de las condiciones para examinarse ante posibles incidencias. Para incidencias son aisladas (con pocos alumnos) se puede: reprogramar un examen oral a los afectados (medida disuasoria para los ‘falsos incidentes’), dar medidas de gracia o corregir sobre lo presentado hasta la incidencia (sólo si no hay vuelta atrás en las preguntas). Conviene

mantener un canal de comunicaciones redundante con los estudiantes para atender incidencias (no para resolver dudas del examen). Es conveniente que todos los profesores de la asignatura estén disponibles en ese canal, en previsión de incidencias generalizadas

EXPERIENCIA EN EL DEPARTAMENTO DE INGENIERÍA TELEMÁTICA

Se ha realizado una experiencia de evaluación telemática en la asignatura Estructura y Protocolos de Redes Públicas, obligatoria del plan de estudios del Grado en Ingeniería de las Tecnologías de Telecomunicación. Esta asignatura cuenta con 190 alumnos matriculados en el curso 2019-2020, y evalúa en la primera convocatoria mediante evaluación continua. Para ello se realizan 3-4 controles de progreso tipo E3 no eliminatorios de materia y en horario y aula de clase, y un control de progreso final tipo E5.1 en aula de examen, todos síncronos. Por motivos prácticos, dada la concentración de alumnos, no se permite el uso de libros o apuntes. El tiempo suele ser holgado. La calificación se obtiene con una suma ponderada con pesos crecientes de las calificaciones parciales.

En este curso ya se realizó un primer control presencial en aula, con 155 presentados (82%) y un 29% de éxito. En los dos cursos anteriores, y para el primer control, la tasa de presentados fue del 80% y el 84% y la de éxito el 20% y el 26%

El segundo control se realizó el 21 de abril por medios telemáticos en modalidad E3, y los días 22 y 23 se realizó una encuesta de satisfacción anónima y voluntaria a los estudiantes. Hubo 156 presentados con un 34% de éxito y la encuesta fue respondida por 100 alumnos (es el límite de respuestas del servicio de encuestas gratuito utilizado).

Para mitigar los riesgos en el segundo control de progreso se han empleado las siguientes contramedidas:

- Riesgo técnico: una prueba previa (examen de chequeo –contramedida: **Verificación Previa** -) donde se les preguntaba a los alumnos 2 preguntas triviales. También se mantuvo abierta una conexión tipo chat de control de incidencias durante el examen –contramedida: **Conexión de Control del Profesor** -. El examen fue realizado en modo alumno por 2 profesores antes de publicarlo para buscar posibles fallos en la implementación.
- Riesgo de confiabilidad: se ha realizado un examen tipo E3 con una tasa de reutilización alta con los controles 1 (tiempo ajustado, inicialmente 20 minutos), 2 (*password*), 3 (conurrencia, preguntas elegidas aleatoriamente y orden de respuestas aleatorio), 4 (preguntas mostradas de 1 en 1 y sin vuelta atrás ni resumen final-) y 11 (recopilar incidencias de incidentes). Las preguntas eran de respuesta de opción única y cada fallo resta un acierto (la calificación esperada de un contestador aleatorio es 0). Se permitía el uso todo tipo de material, dada la imposibilidad de controlarlo, pero el tiempo ajustado hacía complicada su consulta.

Por facilidad de importación del banco de preguntas preexistente (más de 300 preguntas, que combinan texto y figuras) el examen se ha realizado en el servidor *Moodle* hospedado en el Departamento de Ingeniería Telemática. Los alumnos entraban en el aula virtual de *ev.us.es* (*Collaborate*) en el horario de clase para tener una vía de comunicación separada en caso de problemas. En los primeros 15 minutos se les informó de las condiciones del examen y se esperó a que el número de alumnos fuera suficiente. La clave de acceso al examen fue proporcionada justo a la hora de inicio por 2 canales distintos: *ev.us.es* (en imagen) y el foro de *Moodle*.

La valoración del riesgo efectivamente materializado es la siguiente:

- Riesgo técnico: los alumnos manifestaron y los profesores verificaron incidencias técnicas, especialmente al comienzo del test. Estas fueron:
 - Desconocimiento de la clave (1%)
 - Retraso en el acceso (46%)
 - Poca interactividad (65%), reflejada en la lentitud en la carga de cada pregunta.
 - Solo un 16% no tuvo problema alguno
- Riesgo de confiabilidad: de los datos de rendimiento comparados no se observaron indicios de falta de probidad .

Con el fin de obtener información adicional, se procesaron los registros del servidor de *Moodle* que ofrecen información sobre el instante de tiempo y duración de la conexión de cada alumno. Con estas evidencias se pudo identificar a los alumnos que efectivamente comenzaron tarde, los que sufrieron reinicios y los que tuvieron un tiempo anómalamente bajo de examen.

Por su parte, la encuesta reveló que la práctica totalidad de los alumnos utilizaron un PC/portátil, y que un 7% de los alumnos tiene un acceso a Internet que podría ser problemático..

Algunas conclusiones que se sacaron son:

- No ha existido una materialización significativa del riesgo de confiabilidad en el examen. Las contramedidas en su mayoría parecen acertadas con las siguientes precisiones:
 - El tiempo de examen (T) es difícil de ajustar a priori. El alumno con éxito más rápido empleó menos de 10 minutos, mientras que la calificación más alta corresponde a otro que empleó todo el tiempo disponible. El percentil 50 entre los aprobados empleó menos de 20 minutos. Por otro lado los incidentes técnicos tienen un gran impacto si el tiempo es breve. Por ello es recomendable dar un pequeño margen o tener previsto la ampliación del tiempo ante incidencias. La clave de comienzo del test no era necesaria, pues los alumnos no pudieron acceder al test antes de la hora de comienzo y es superflua si se cuenta con la clave de acceso al sistema.
 - La navegación secuencial estricta en las preguntas crea ansiedad en los estudiantes, que encuentran dificultades en la gestión del tiempo restante. Por ello es recomendable bien permitir la navegación libre, combinada con una tasa de reutilización baja (aumentando el banco de preguntas), bien ajustar el tiempo de forma más holgada, pero no tanto que permita la consulta indiscriminada o la colaboración con otros alumnos o con terceros.
- Deben tomarse nuevas medidas para reducir el riesgo técnico:
 - Debe relajarse la concurrencia, que es una exigencia en controles presenciales pero no en los telemáticos. Los alumnos se incorporarían a la prueba de forma gradual y su tiempo computaría a partir de ese momento. El intervalo de acceso no debe extenderse hasta suponer una realización sin concurrencia
 - Debe reducirse el peso de las imágenes
 - Fortalecer la capacidad del servidor de *Moodle* o (preferentemente) pasar a *ev.us.es*
 - Algunos alumnos tuvieron problemas locales de acceso a Internet, por lo que se recomienda informar al alumno para que realice: **Ajuste Red Local**.
 - Algunos alumnos tuvieron problemas para obtener la clave de comienzo. Cuando se use esta medida de control, poner en las instrucciones del test la clave de comienzo.

Tras analizar la situación y las alternativas se ha decidido repetir la prueba con todas las mejoras anteriormente expuestas y tomar la mejor calificación entre ambas oportunidades. Se ha dado realimentación continua al alumnado de todo este proceso y se percibe que mayoritariamente valoran los esfuerzos que se están realizando, por lo que parece buena idea el realizar una consulta para ver las incidencias tras el examen.

Para el resto del curso la planificación propuesta es realizar otro tercer control de este tipo, y un control final de tipo E5.4 o E5.3 con muy baja tasa de reutilización que se contestaría en papel y se entregaría digitalmente. La implementación definitiva y las contramedidas a usar están por decidir.

LIMITACIONES DE ESTE TRABAJO

Este es un trabajo preliminar que está en continua evolución y como tal, adolece de algunas limitaciones que conviene saber.

- La limitación más notoria es que sólo considera el escenario de *Blackboard* contratado por la Universidad de Sevilla como única posibilidad de realización de evaluaciones. En los dos tipos de riesgo considerado, tecnológico y de confiabilidad, a buen seguro el avezado profesor de ingeniería podrá encontrar modos de fraude no considerados o nuevas contramedidas no tenidas en cuenta.
- Hay formas de examinar¹² y herramientas de supervisión asociadas a la plataforma *Blackboard* que no han sido consideradas, pues en el momento de realizar este informe no se encuentran disponibles en *ev.us.es*. Ejemplos de estas herramientas son: *Respondus Lock Browser* (que bloquea el navegador web del alumno

¹² Las Pruebas de evaluación competitiva (PEC), donde la calificación de la prueba se determina de forma comparativa, no absoluta, de forma que la ventaja de un alumno implique una pérdida para quien lo ayude, desincentivando la colaboración entre alumnos para resolver la prueba

ante comportamientos sospechosos, para limitar la suplantación de identidad –vector V2-) o *Examity* (que se está integrando en *ev.us.es* para una finalidad similar). Este tipo de herramientas pueden tener problemas de aceptación por parte del alumnado (derecho a la intimidad) y con el tratamiento de datos (RGPD). Las herramientas *Keylogger*¹³, capturan el comportamiento del alumno frente al ordenador (teclas pulsadas y movimientos del ratón en cada momento, ventanas utilizadas, etc...) y podrían ser de utilidad para detectar comportamientos anómalos y tener evidencias ante un caso de falso incidente. En futuras versiones de este trabajo se podrían incorporar estas nuevas herramientas, aunque ya se han apuntado mecanismos que permitirían hacerlas menos efectivas.

Estas limitaciones, no obstante, pensamos que no invalidan la principal contribución del trabajo, que no es otra que ofrecer una panorámica de los riesgos inherentes a la evaluación telemática, así como una lista (a buen seguro incompleta) de contramedidas, que facilite a cada profesor la toma de decisiones bien fundadas sobre qué hacer en su asignatura.

CONCLUSIONES

Es imposible suprimir el riesgo en un examen telemático, como también lo es en un examen presencial. De forma natural, los exámenes telemáticos abren un mayor número de oportunidades a quien desea sortear las normas establecidas. Todos los actores deben ser conscientes de estos riesgos. Los profesores se enfrentan al desafío de implementar mecanismos de evaluación confiables, los alumnos tendrán que aceptar nuevas formas de implementar y monitorizar esta evaluación y la Universidad deberá dotarse no sólo a sí misma y a los profesores, sino también a los alumnos con necesidades especiales con la necesaria infraestructura técnica y soporte normativo. Está por ver si el coste será razonable para todos.

Con independencia de las orientaciones para el uso de contramedidas que se han ofrecido en este trabajo, con carácter general se recomienda:

- La realización de varias pruebas de distintos tipos, con una ponderación inversamente proporcional al nivel de riesgo de cada una. Un caso práctico podría ser:
Ex1: (E2 / 1,3,4,5,6) 15% calificación
Ex2: (E3 / 1,3,4,6,7) 25% calificación
Ex3: (E5.4 / 1,2, 4, 5) 60% calificación
- Es conveniente verificar el entorno del examen con el alumno antes de realizarlo. Realiza el examen en modo alumno para verificar posibles errores de comportamiento. Antes del examen hacer una pequeña prueba (contramedida **Verificación Previa**) para practicar la mecánica (información de la dinámica del examen, controles a realizar, acceso a Internet, navegador, etc).
- Es conveniente pedir realimentación de la prueba a los alumnos: una encuesta de satisfacción con el examen, problemas encontrados con los controles, tipo de acceso, equipos desde el que lo ha realizado, incidencias, etc... permite ajustar mejor los parámetros para el siguiente control y modular posibles medidas compensatorias (si las hubiere). Ver Anexo II.
- Debe informarse al alumno convenientemente de las condiciones del examen.

Para finalizar debemos señalar que no existe una solución mágica que todos los profesores puedan aplicar universalmente¹⁴. Cada profesor debe encontrar la mejor forma de evaluar el grado de dominio de la materia de nuestros alumnos, alcanzando un compromiso entre los recursos que va a dedicar a examinar y la reducción del riesgo que somos capaces de aceptar en las actuales circunstancias.

¹³En <https://sourceforge.net/projects/basickeylogger/> hay un software open source keylogger muy simple para Windows (no requiere instalación). Existen proyectos similares en Linux, Mac, Android, etc...

¹⁴ Esta misma conclusión está presente en el reciente documento del 26 de marzo de 2020 sobre experiencias de modelos de evaluación alternativos CRUE (disponible en: <https://www.us.es/sites/default/files/comunicacion/coronavirus/resumen-jornada-modelos-evaluacion.pdf>)

ANEXO I: CONSIDERACIONES PARA LA CREACIÓN DE LOS TIPOS DE EXÁMENES INDICADOS Y LAS CONTRAMEDIDAS PROPUESTAS

Blackboard permite realizar básicamente dos tipos de pruebas: tipo exámenes y tipo actividad (ayuda disponible en: https://help.blackboard.com/es-es/Learn/Instructor/Tests_Pools_Surveys)

A modo de resumen, para crear un contenido tipo **examen** los pasos a dar serán:

- 1) (opcional) Crear un banco de preguntas (gestión de curso/herramientas de curso/Bancos de preguntas)
 - a. Desarrollarlo
 - i. Se le pone un nombre (puede ser una categoría: preguntas tema1)
 - ii. Se crean las preguntas (cuestionarios cortos, elección múltiple, verdadero/falso, redacción – texto libre-, subir fichero, etc...) (en cada pregunta se puede indicar si las respuestas se muestran en orden aleatorio -contramedida **Random Answer**-
 - iii. Se pueden importar desde un fichero de texto plano separado con tabulaciones (ver la ayuda). Este fichero de texto se puede crear fácilmente a partir de una hoja Excel. Un problema es que no admite imágenes¹⁵.
 - b. Importarlo
 - i. Desde otro curso o asignatura donde se encuentre, o bien en un formato denominado QT12.1 (formato complejo con varios ficheros en xml)¹⁶.
- 2) Crear un examen (gestión de curso/herramientas de curso/examen)
 - a. Desarrollarlo (lienzo del examen)
 - i. Se pueden crear preguntas (igual que el punto 1.a.ii)
 - ii. Se pueden reutilizar de un banco de preguntas, otros exámenes, etc... Existe la opción de 'crear bloque aleatorio' que permite seleccionar preguntas de un banco elegidas aleatoriamente en el momento del examen (contramedida **Random Question**) y seleccionar el número de preguntas que componen dicho bloque.
 - iii. En 'configuración de la pregunta' se puede elegir si queremos aleatorizar las respuestas (contramedida **Random Answer**)
 - iv. Sobre el lienzo de examen se van añadiendo preguntas o bloques de preguntas hasta finalizar.
- 3) Crear un contenido de examen: Contenidos/Evaluaciones/Examen
 - a. Se especifica el examen que se quiere poner (previamente creado)
 - b. Se especifican las opciones, entre ellas:
 - i. Permitir 1 o varios intentos (por defecto sólo 1)
 - ii. Temporizador y envío automático (contramedida **Tiempo**)
 - iii. Mostrar desde (fecha/hora en la que los alumnos tendrán disponible el examen).
Contramedida **Concurrencia**
 - iv. Contraseña (para acceso al examen. Contramedida **Password**)
 - v. Restringir ubicación (filtro IP)
 - vi. Excepciones de disponibilidad de examen: permite entregar el examen a un determinado grupo o alumnos (contramedida **BC**)
 - vii. Fecha de vencimiento (contramedida **Tiempo**)
 - viii. Mostrar resultados al estudiante. Se puede desactivar esta opción para aplicar la contramedida **SingleNoSummary**.
 - ix. Presentación del examen: preguntas de una en una (**SingleNoSummary**) y no está permitida la vuelta atrás (**NoBack**)
 - x. Preguntas en orden aleatorio (**Random Query**)

¹⁵ Una alternativa para importar preguntas de texto con preguntas puede ser: importar preguntas de texto con una etiqueta (por ejemplo: LABEL1), exportar el fichero en QT12.1 desde *Blackboard*, modificar dicho fichero para que sustituya las etiquetas por imágenes fichero –herramienta en desarrollo actualmente- y por último volverlo a importar.

¹⁶ Hasta la fecha no se ha conseguido encontrar cómo pasar un banco de preguntas con imágenes de otra plataforma (tipo *Moodle*) a formato QT12.1 para poder importarlo en *ev.us.es*

En *Blackboard* también podemos crear una **actividad** (contenidos/evaluaciones/actividad), en la que se especifican:

- 1) Fecha de vencimiento (día/hora), y disponibilidad para los alumnos (permiten **Concurrencia y Tiempo**)
- 2) Número de intentos (uno, por defecto)
- 3) Utilizar herramienta anti-plagio (contramedida **SafeAssign**). Más información en ver <https://help.blackboard.com/es-es/Learn/Instructor/Assignments/SafeAssign>

USO DE SMOWL EN LOS EXÁMENES

Para utilizar **Smowl** durante el examen, tendremos que:

- Habilitarlo: Personalización / disponibilidad de herramientas
 - Habilitar las pestañas de Smowl (todas)
- Activar su funcionamiento durante el examen:
 - Smowl Curso / Examen, seleccionar el examen o tarea a vigilar
- Tras el examen, se pueden ver los resultados y alumnos registrados.

IMPLEMENTACIÓN DE EXÁMENES DE DIVERSOS TIPOS

Para implementar exámenes tipo E1, E2, E3:

- Utilizar contenidos tipo examen con las opciones explicada
- La importación de preguntas con imágenes desde otras plataformas (*Moodle*) tiene cierta complejidad.

Para implementar exámenes tipo E4:

- Existen varias alternativas
 - Crear un banco de preguntas, realizar una asignación distinta a cada examen y asignar un examen a cada alumno (Examen E4)
 - Se pueden generar diferentes preguntas con texto utilizando herramientas (excel – función sustituir- o word –combinar correspondencia-), y luego importar las preguntas.
 - La asignación de un examen a cada alumno es una tarea muy tediosa cuando el número de alumno es grande
 - Crear un banco de preguntas y realizar la asignación de preguntas de forma aleatoria (exámenes tipo E3). Podemos emplear las técnicas anteriores para crear grandes bancos de pregunta, donde la probabilidad de repetir preguntas sea muy baja (sería parecido a un examen E4, pero más fácil de gestionar la asignación de exámenes a los alumnos).
 - Utilizar preguntas con datos parametrizados (en función de su mes de nacimiento, los dígitos de su dni, ...).
 - calificar de forma automática: en una Excel donde se exportan las respuestas de los alumnos
 - calificar de forma manual: desde *Blackboard* observando las respuestas de los alumnos

Para implementar exámenes tipo E5.1, E5.2 y E5.3 disponemos de tres alternativas

- Utilizar un examen con preguntas de respuesta tipo *fichero*. Esto nos permite aplicar todos los controles y medidas asociadas a los exámenes anteriormente vistas. Tiene como ventajas que el alumno libremente puede hacer fórmulas, dibujos, etc... un desarrollo completo, pero como inconveniente que debe digitalizarse el resultado (foto con el móvil) antes de entregarlo. También puede entregarse un fichero pdf generado con Word u otro editor.
- Utilizar un examen con preguntas tipo examen de *redacción*. En este caso evitamos la digitalización a costa de complicar y limitar los contenidos del desarrollo (el editor permite texto, tablas y ecuaciones) e incrementar el tiempo de examen.
- Utilizar un contenido tipo *actividad*, en el que se le proporciona el enunciado del examen. Esto limita el número de controles pero si permite utilizar **SafeAssign**.

En los exámenes donde existe un enunciado diferente para cada alumno (exámenes E.4 y E5.4), existen dos problemas que deben ser abordados:

- La creación de los enunciados o exámenes individuales:
 - Se pueden crear tantos exámenes como alumnos... (gran coste)

- Se puede automatizar la creación de exámenes diferentes:
 - Para crear test de preguntas: generar los ficheros de preguntas en texto e importarlos. Existen muchas alternativas para conseguir esto. Con Word (combinar correspondencia) o con un script de Linux que utilice los comando sed/awk o incluso con excel¹⁷.
 - Para generar enunciados de exámenes en pdf se puede, además de usar combinación de correspondencia en Word, crear una plantilla del examen en Latex, realizar las sustituciones pertinentes para cada examen en función de una hoja de cálculo (puede ser en texto csv) y compilarlos automáticamente para tener diferentes enunciados en pdf. Ver ejemplo descrito al final de esta página.
- La entrega a los alumnos: existen las siguientes alternativas
 - Enviar por correo electrónico a cada alumno su enunciado. Se puede realizar de dos formas
 - Automatizada con una herramienta. Se puede implementar dicha herramienta en Linux para automatizar el envío del examen a una lista que contendrá el email del alumno y su examen (tener en cuenta el tiempo entre correos para no ser detectado como *spam*). Esto incide en la **conurrencia**, que tendría que implementarse con mayor margen, repartiendo el examen, al menos, 20 minutos antes del comienzo. Se podría verificar en *Collaborate* /un chat de control / email que todos los alumnos han recibido el examen 10 minutos antes del comienzo y reenviarlo a alguna dirección alternativa a aquellos que tuvieran problemas. Para implementar concurrencia, el examen podría ir con clave de cifrado (contramedida –**Password**- en zip viene implementado) y ofrecerles dicha clave en la hora de comienzo.
 - Manual:
 - Desde *Blackboard* notificando a cada alumno con un correo y adjuntando el enunciado. Es posible cifrar el fichero del examen y distribuir la clave al comienzo.
 - Realizando tantos exámenes como alumnos y asignándolos de forma individual a los diversos alumnos o grupos de alumnos. De esta forma se puede fijar la misma hora de comienzo a todos.
 - Realizar tantos exámenes como alumnos (cada uno con su enunciado) y realizar una asignación individual a cada alumno desde *BlackBoard*.

A modo de ilustración se ponen a continuación ejemplo de una sustitución en Latex que genera tantos exámenes personalizados en pdf como indique el fichero de sustituciones.

Fichero: plantilla.tex

```
\documentclass[a4paper,12pt]{article}
\begin{document}

Examen de ejemplo.
Código examen: LB0
Alumno: LB1
Indique la raíz cuadrada del número LB2

\end{document}
```

Fichero: sustituciones.csv

(se puede generar a partir de un fichero excel con la lista de clase guardado como csv)

```
id-examen (LB0); Alumno (LB1); numero(LB2)
ex1;Fulano;343
ex2;Mengano;889
ex3;Zutano;666
```

¹⁷ Un ejemplo muy rudimentario con excel sería: copiar una pregunta en N filas (p.e. cuánto es LB1+ 5?). En cada fila de la excel se pone un código de Di dígitos de control: que pueden valer 0,1,2, ... y se define una sustitución para cada uno (por ejemplo: SI(D1=0;sustituir(PREGUNTA; LB1;"5");sustituir(PREGUNTA;LB1;"6")). Por cada dígito de control se realiza una sustitución sobre el resultado anterior y obtendremos preguntas tipo: cuánto es 5+2? Cuánto es 6+2? etc... esta misma técnica se puede emplear para las respuestas. Al final copiar en una hoja con formato válido en *Blackboard* y exportar a csv separado por tabulaciones

Fichero: generar.sh

```
echo "inicio del proceso de generación"
for ((i=1; i<=3; i++))
do

    excode="ex$i"
    id=$(egrep "$excode" sustituciones.csv | awk -F ";" '{print $1}')
    alumno=$(egrep "$excode" sustituciones.csv | awk -F ";" '{print $2}')
    numero=$(egrep "$excode" sustituciones.csv | awk -F ";" '{print $3}')
    echo "generando examen $id $alumno $numero"
    sed 's/LB0 /'$id'/' < plantilla.tex > aux.tex
    sed 's/LB1 /'$alumno'/' < aux.tex > aux2.tex
    sed 's/LB2 /'$numero'/' < aux2.tex > aux.tex

    latex aux.tex
    dvips aux.dvi
    mv aux.dvi $excode.dvi
    dvi2pdf -o $excode.pdf $excode.dvi
    rm $excode.dvi
done
```

Con este ejemplo, en un entorno bien configurado (e.g., Linux y LaTeX instalado), ejecutando *genera.sh* se crearían los exámenes: *ex1.pdf*, *ex2.pdf* y *ex3.pdf*, cada cual con sus datos correspondientes según las sustituciones. Nótese que con una pequeña modificación al final de *genera.sh* se podrían enviar a los alumnos los exámenes por email tan sólo con tener su dirección de correo en el campo correspondiente del fichero: *sustituciones.csv*

Los exámenes tipo E7 (trabajos) se podrían realizar como actividad (permite utilizar la herramienta anti-plagio **SafeAssign**) o como examen de entrega de un fichero.

ANEXO II: MODELO DE ENCUESTA DE REALIMENTACIÓN

Las cuestiones están abiertas a todos los alumnos, independientemente de si concurren o no al examen.

1. Cuestiones previas al examen:
 - 1.1. Dispuse de información exacta de las condiciones y momento del examen (V/F)
 - 1.2. Se suministraron instrucciones de configuración del entorno de realización (V/F)
 - 1.3. Realizaste pruebas con el entorno (plataforma, equipos propios) (V/F)
2. Cuestiones sobre las situación del alumno frente al examen:
 - 2.1. ¿Qué dispositivo usaste para el control (simple)
 - PC,
 - móvil,
 - tablet,
 - Otro
 - 2.2. El dispositivo que usaste es
 - De uso propio exclusivamente
 - De uso compartido con otros miembros de la familia
 - 2.3. ¿Con qué tipo de acceso a Internet lo hiciste? (simple)
 - Fibra (>30Mb/s),
 - ADSL (hasta 16Mb/s),
 - Cobertura 4G,
 - Cobertura 3G,
 - Otro
3. Cuestiones sobre la celebración del examen:
 - 3.1. ¿Qué tipo de problemas ****técnicos**** encontraste durante la realización del control? (múltiple)
 - Retraso al acceder
 - Cortes en la conexión
 - Retraso al cambiar de página
 - Ninguno
 - Otro
 - 3.2. El tiempo del ejercicio resultó:
 - Insuficiente debido exclusivamente a los problemas técnicos
 - Insuficiente independientemente de los problemas técnicos
 - Suficiente pero muy ajustado
 - Suficiente
 - Sobrado
 - 3.3. ¿Dispusiste de un canal de comunicaciones durante el examen para informar de problemas o incidencias? (V/F)
4. Cuestiones sobre la valoración del examen
 - 4.1. ¿Considera que la prueba, en las condiciones en que lo ha realizado, estima adecuadamente sus conocimientos? (escala 1-5)
 - 4.2. ¿Considera que la prueba, en ausencia de problemas técnicos, estimaría adecuadamente sus conocimientos? (escala 1-5)
 - 4.3. Ha superado el examen? (V/F)
5. ¿Qué aspectos positivos, si hay alguno, destacaría? (libre)
6. ¿Qué aspectos negativos considera más relevantes? (libre)28/4/2020