Activo	Asignación de Tareas
Amenazas	(1) Eliminación no deseada de la asignación. (2) Modificación no deseada de la asignación. (3) Envío de una asignación a un alumno suplantando al profesor. (4) Repudio de la asignación recibida. (5) Envío de la asignación a una persona no matriculada en el curso. (6) Visualización de la asignación por una persona ajena al curso. (7) Imposibilidad de acceso a la asignación.
Exposición	**(1) Eliminación no deseada de la asignación** La eliminación de la asignación de tareas durante el desarrollo del curso académico, sea de manera accidental o sea de manera deliberada y malintencionada, tendría un impacto notable sobre el sistema. Al no disponer de la asignación de tareas, mientras ésta se reconstruye, puede que hubiese que cancelar una o dos clases. Además, se perdería cierto tiempo en reconstruir la asignación perdida. Incluso esta asignación podría llegar a perderse completamente en caso de no se hubiesen guardado copias. La eliminación de la asignación de manera accidental por un error humano nunca es descartable. Además, la eliminación malintencionada y deliberada tampoco es descartable, ya que los alumnos, en un momento determinado del curso, pueden estar agobiados o sobrecargados de trabajo, viéndose tentados de eliminar la asignación de tareas para así poder ganar algo de tiempo. Por otro lado, el intento de eliminación de la asignación de tareas por parte de terceras personas ajenas a la asignatura se considera improbable. Por tanto, a tenor de estas argumentaciones, *la exposición a esta amenaza se considera alta*. **(2) Modificación no deseada de la asignación** La modificación de la asignación de tareas durante el desarrollo del curso académico, sea de manera accidental o sea de manera deliberada y malintencionada, tendría un impacto notable sobre el sistema. Al no coincidir la asignación de tareas con la originalmente creada podrían producirse problemas durante el desarrollo de las clases. Dependiendo de la amplitud de las modificaciones, podría ser necesario incluso cancelar una o dos clases mientras se consigue reconstruir la asignación original. La asignación original podría incluso llegar a perderse completamente en caso de no se hubiesen guardado copias y no se sepa cómo revertir las modificaciones. La modificación de la asignación de manera accidental por un error humano nunca es descartable. Además, la modificación malintencionada y deliberada tampoco es descartable, ya que los alumnos, en un momento determinado del curso, pueden estar agobiados o sobrecargados de trabajo, viéndose tentados de eliminar la asignación de tareas para así poder ganar algo de tiempo. Por otro lado, el intento de modificación de la asignación de tareas por parte de terceras personas ajenas a la asignatura se considera improbable. Por tanto, a tenor de estas argumentaciones, *la exposición a esta amenaza se considera alta*.

(3) Envío por correo de una asignación a un alumno suplantando al profesor

En este caso, un alumno recibiría un correo que pareciese procedente del profesor de la asignatura, pero con una asignación de tareas falsa. Esto podría confundir al alumno, el cual, si lo diese por verdadero, podría llegar a realizar una serie de tareas en balde, ya que nunca le fueron solicitadas. Si el número de alumnos afectados por esta suplantación de personalidad fuese alto, el impacto sobre la asignatura podría ser significativo. No obstante, se considera improbable que un alumno, o una tercera persona, se tome las molestias necesarias para suplantar la personalidad del profesor con este fin. Sí sería más probable que un alumno, con el objetivo de sortear diversas tareas, tratase de falsificar un correo electrónico del profesor para alegar que la asignación de tareas que él ha recibido es distinta de la que le reclama el profesor.

Por tanto, a tenor de estas argumentaciones, *la exposición a esta amenaza se considera media*.

(4) Repudio de la asignación recibida

Un alumno, con el objetivo de evitar o postergar la realización de diversas tareas, podría alegar no haber recibido la asignación de tareas por correo, o alegar haber recibido una diferente. Esta posibilidad es bastante plausible. Si lo alumnos pudiesen repudiar con facilidad tareas, el desarrollo normal de la asignatura se complicaría bastante, ya que la organización del día a día se vería muy resentida.

Por tanto, a tenor de estas argumentaciones, *la exposición a esta amenaza se considera alta*.

(5) Envío de la asignación a una persona no matriculada en el curso

Por algún tipo de error accidental, podría enviarse una asignación de tareas a un destinatario diferente al alumno que debe realizar dichas tareas. Si el sistema está bien diseñado, este error se considera bastante improbable. Por otro lado, se considera que la asignación de tareas no es información personal sensible, por lo que a priori no se considera que este error pueda producir perjuicios importantes, ni al alumno objeto de la filtración de información, ni al sistema.

Por tanto, a tenor de estas argumentaciones, *la exposición a esta amenaza se considera muy baja* y no se continuará con su análisis.

(6) Visualización de la asignación por una persona ajena al curso

Por algún tipo de error accidental, podría hacerse la asignación de tareas accesible a un alumno no matriculado en la asignatura. Dado que se considera la asignación de tareas como información personal no sensible, se entiende que este error no produce perjuicios importante ni a los alumnos objetos de esta filtración de información ni al sistema.

Por tanto, a tenor de estas argumentaciones, *la exposición a esta amenaza se considera muy baja* y no se continuará con su análisis.

	(7) Imposibilidad de acceso a la asignación Por algún tipo de error o circunstancia accidental, la asignación de tareas podría quedar temporalmente inaccesible a los alumnos matriculados en la asignatura. Si esta inaccesibilidad fuese prolongada y no puntual, podría impedir a los alumnos desarrollar sus tareas a tiempo, por lo que podría ser necesario cancelar una o más clases, obligando a rediseñar el calendario de la asignatura. Por otra parte, la vida está llena de imprevistos y circunstancias excepcionales que podrían impedir el acceso al sistema, por lo que la posibilidad de que la asignación quede inaccesible siempre existe. Por tanto, a tenor de estas argumentaciones, *la exposición a esta amenaza se considera alta*.
Potenciales Ataques	**(1) Eliminación no deseada de la asignación** *Ataque 1.1: Eliminación por error.* El profesor, de manera no intencionada, debido por ejemplo al cansancio por una saturación de trabajo, elimina sin darse cuenta o ser consciente de ello la asignación de tareas creada, o la deja de algún modo inaccesible a los alumnos. Por ejemplo, si el sistema lo permite, podría ocultarla. *Ataque 1.2: Sesión abierta y eliminación por azar.* El profesor deja una sesión del sistema abierta en un dispositivo, alguien accede a ella y de manera accidental elimina la asignación. Por ejemplo, el profesor podría acceder al sistema desde un dispositivo móvil, guardar dicho dispositivo en su bolsillo o en una maleta, provocando que se generen una serie de pulsaciones y eventos aleatorios sobre el sistema que podrían acabar en la eliminación de la asignación creada. Otro escenario sería que el profesor esté trabajando en su PC desde casa, abandone un momento el PC para ir al baño o a la cocina, una de sus hijas o hijos menores aparezca por el despacho o zona de trabajo y de manera no intencionada o aleatoria, elimine la asignación de taras del curso en el que estaba trabajando. *Ataque 1.3: Sesión abierta y eliminación intencionada.* El profesor deja una sesión del sistema abierta en un dispositivo, permitiendo que un tercero acceda a ella, el cual aprovecha la ocasión para eliminar la asignación de tareas del curso, entre otras posibles maldades. Por ejemplo, el profesor podría dejar la puerta de su despacho abierta mientras va al baño, un alumno aprovechar para entrar y colarse en dicho despacho, acceder al PC y eliminar la asignación. De igual forma, el profesor podría dejar el sistema abierto en un computador de algún aula o laboratorio del centro donde imparta clases de manera que un alumno pueda acceder al sistema y eliminar la asignación. *Ataque 1.4: Robo de credenciales y eliminación.* Un tercero, normalmente un alumno, se hace por medio de algún mecanismo que desconocemos, con las credenciales de acceso al sistema del profesor y elimina la

asignación de tareas.

NOTA: Este ataque se especifica no para tratar de evitar el robo de credenciales, tarea de la que se deberá encargar el análisis de seguridad del activo *credenciales*, sino para poder recuperarnos de este ataque en caso de que, por el motivo que sea, alguien consiga saltarse todas las medidas de control ideadas para la protección de las credenciales y pueda llevarlo a cabo.

Ataque 1.5 Fallo del soporte físico donde se aloja la asignación.

El soporte físico donde se aloja la asignación sufre algún tipo de defecto físico o lógico que impide el correcto acceso a los datos de la aplicación.

(2) Modificación no deseada de la asignación

Ataque 2.1: Modificación por error.

El profesor, de manera no intencionada, debido por ejemplo al cansancio por una saturación de trabajo, modifica sin darse cuenta o ser consciente de ello la asignación de tareas creada. Igualmente, también por fatiga, podría realizar una serie de cambios que no fuesen correctos.

Ataque 2.2: Sesión abierta y modificación por azar.

El profesor deja una sesión del sistema abierta en un dispositivo, alguien accede a ella y de manera accidental elimina la asignación. Por ejemplo, el profesor podría acceder al sistema desde un dispositivo móvil, guardar dicho dispositivo en su bolsillo o en una maleta, provocando que se generen una serie de pulsaciones y eventos aleatorios sobre el sistema que podrían modificar la asignación de tareas de manera aleatoria. Otro escenario sería que el profesor esté trabajando en su PC desde casa, abandone un momento el PC para ir al baño o a la cocina, una de sus hijas o hijos menores aparezca por el despacho o zona de trabajo y de manera no intencionada o aleatoria, elimine la asignación de taras del curso en el que estaba trabajando.

Ataque 2.3: Sesión abierta y modificación intencionada.

El profesor deja una sesión del sistema abierta en un dispositivo, permitiendo que un tercero acceda a ella, el cual aprovecha la ocasión para modificar la asignación de tareas del curso, entre otras posibles maldades. Por ejemplo, el profesor podría dejar la puerta de su despacho abierta mientras va al baño y un alumno podría aprovechar para entrar y colarse en dicho despacho, acceder al PC y modificar la asignación. De igual forma, el profesor podría dejar el sistema abierto en un computador de algún aula o laboratorio del centro donde imparta clases de manera que un alumno pueda acceder al sistema y eliminar la asignación.

Ataque 2.4: Robo de credenciales y modificación.

Un tercero, normalmente un alumno, se hace, por medio de algún mecanismo que desconocemos, con las credenciales de acceso al sistema del profesor y modifica la

asignación de tareas.

NOTA: Este ataque se especifica no para tratar de evitar el robo de credenciales, tarea de la que se deberá encargar el análisis de seguridad del activo *credenciales*, sino para poder recuperarnos de este ataque en caso de que, por el motivo que sea, alguien consiga saltarse todas las medidas de control ideadas para la protección de las credenciales y pueda llevarlo a cabo.

(3) Envío de una asignación a un alumno suplantando al profesor.

Ataque 3.1: Configuración y envío de un correo tipo pishing*.*

Un alumno con ciertos conocimientos de *hacking* compone y envía un correo suplantando la identidad del profesor con una nueva asignación de tareas a uno o más alumnos, o notificando modificaciones a la asignación ya existente.

Ataque 3.2: Obtención de acceso al PC o similar del profesor y envío de correo.

El profesor deja algún dispositivo personal, como PC o teléfono móvil, accesible, permitiendo así que un tercero pueda utilizarlo. Por ejemplo, el profesor podría dejar la puerta de su despacho abierta mientras va al baño, un alumno aprovechar la ocasión para acceder al PC del profesor, luego a su correo y finalmente enviar una nueva asignación.

Ataque 3.3: Robo de credenciales del correo del profesor y envío de correo.

Un tercero, normalmente un alumno, se hace, por medio de algún mecanismo que desconocemos, con las credenciales del sistema de correo del profesor y envía un correo con una nueva asignación de tareas a uno o más alumnos, o notifica modificaciones a la asignación ya existente.

(4) Repudio de la asignación recibida.

Ataque 4.1: Negación de haber recibido el correo con la asignación de tareas.

Un alumno, por el motivo que fuese, no ha realizado una cierta tarea y para salir de dicha situación alega no haber recibido por correo notificación alguna de las tareas a realizar.

(7) Imposibilidad de acceso a la asignación.

Ataque 7.1: Caída del servidor del servidor del sistema (moodle).

Por algún tipo de fallo hardware o software, el servidor de Moodle no está operativo.

NOTA: La protección del servidor del sistema se realiza en el análisis del activo *servidor*. Este ataque se añade única y exclusivamente para proporcionar mecanismos de recuperación y parcelación de activos en caso de que este ataque llegue a materializarse.

	Ataque 7.2: Caída de las redes de comunicación. Por algún tipo de fallo hardware o software, las redes de comunicaciones no están operativas. NOTA: La protección de las redes de comunicaciones se realiza en el análisis del activo *redes de comunicación*. Este ataque se añade única y exclusivamente para proporcionar mecanismos de recuperación y parcelación de activos en caso de que este ataque llegue a materializarse. *Ataque 7.3: Saturación del servidor de Moodle.* Por algún tipo de fallo hardware o software, el servidor del sistema está saturado y, o bien directamente no responde, o bien su respuesta es muy lenta. NOTA: La protección del servidor del sistema se realiza en el análisis del activo *servidor*. Este ataque se añade única y exclusivamente para proporcionar mecanismos de recuperación y parcelación de activos en caso de que este ataque llegue a materializarse. *Ataque 7.4: Saturación de las redes de comunicación.* Por algún tipo de fallo hardware o software, las redes de comunicación del sistema están saturadas y, o bien directamente no responden, o bien su respuesta es muy lenta. NOTA: La protección de las redes de comunicaciones del sistema se realiza en el análisis del activo *redes de comunicación*. Este ataque se añade única y exclusivamente para proporcionar mecanismos de recuperación y parcelación de activos en caso de que este ataque llegue a materializarse.
Medidas de Control	**Medida 1: Mostrar un mensaje de alerta que informe de que se va a realizar una eliminación o modificación de la asignación.** Dado que, una vez generada la asignación inicial de tareas, tanto su modificación como su eliminación serán operaciones infrecuentes, se considera que mostrar un mensaje al usuario para alertarlo de que está a punto de llevar a cabo una modificación o una eliminación de la asignación no perjudica a la usabilidad y facilidad de operación general del sistema, contribuyendo además a evitar eliminaciones y modificaciones realizadas. Mitiga: *Ataque 1.1: Eliminación por error* y *Ataque 2.1: Modificación por error*. **Medida 2: Resaltar las modificaciones realizadas a la vez que se pide confirmar una modificación de una asignación.** Si a la vez que pedimos confirmación para realizar una serie modificaciones, conseguimos resaltar de alguna manera las modificaciones que se van a realizar, se facilita que el usuario pueda revisarlas antes de confirmarlas, lo que contribuiría a reducir las modificaciones erróneas debidas a errores o descuidos humanos no intencionados.

Mitiga: *Ataque 2.1: Modificación por error*.

Medida 3: Solicitar las credenciales del profesor antes de realizar una operación de modificación o eliminación de la asignación.

Dado que, una vez generada la asignación inicial de tareas del curso, tanto su modificación como su eliminación serán operaciones infrecuentes, se considera que solicitar de nuevo las credenciales al usuario para confirmar que el que va a realizar la operación es realmente el usuario y no un tercero suplantándolo no perjudica a la usabilidad y facilidad de operación general del sistema. Además, se considera que la solicitud de una contraseña dificulta que la asignación se pueda eliminar o modificar por azar. Por ejemplo, a consecuencia de guardar un dispositivo móvil sin bloquear en un bolsillo o maleta.

Mitiga: *Ataque 1.2: Sesión abierta, y eliminación por azar*, *Ataque 1.3: Sesión abierta y eliminación intencionada*, *Ataque 2.2: Sesión abierta y modificación por azar* y *Ataque 2.3: Sesión abierta y modificación intencionada.*

Medida 4: Guardar un historial de versiones de la asignación.

Dado que, las asignaciones de tareas son datos ligeros que ocuparán un espacio bastante reducido y, además, una vez generada la asignación inicial de tareas del curso tanto su modificación como su eliminación serán operaciones infrecuentes, se considera que es viable guardar un historial con todas las versiones de la asignación generadas durante un curso académico. Esto contribuiría a restaurar una versión estable de la asignación de tareas en caso de que ésta se dañase por cualquier motivo.

Mitiga: *Ataque 1.1: Eliminación por error, Ataque 1.2: Sesión abierta, y eliminación por azar, Ataque 1.3: Sesión abierta y eliminación intencionada, Ataque 1.4: Robo de credenciales y eliminación, Ataque 2.1: Modificación por error, Ataque 2.2: Sesión abierta y modificación por azar, Ataque 2.3: Sesión abierta y modificación intencionada* y *Ataque 2.4: Robo de credenciales y modificación.*

Medida 5: Enviar un correo al profesor para informarle de que la asignación de tareas ha sido eliminada o modificada.

Dado que, una vez generada la asignación inicial de tareas, tanto su modificación como su eliminación serán operaciones infrecuentes, se considera que enviar un correo al profesor para informarle de que la asignación ha sido modificada o eliminada no generará un envío masivo de correos que puedan resultarle molestos. Por otro lado, esta medida contribuiría a que, si la asignación ha sido modificada o eliminada sin su consentimiento, éste pueda restaurarla a la mayor prontitud posible.

Mitiga: *Ataque 1.2: Sesión abierta y eliminación por azar, Ataque 1.3: Sesión abierta y eliminación intencionada, Ataque 1.4: Robo de credenciales y eliminación, Ataque 2.2: Sesión abierta y modificación por azar, Ataque 2.3: Sesión abierta y modificación intencionada* y *Ataque 2.4: Robo de credenciales y modificación.*

Medida 6: La asignación de tareas se publicará en la plataforma de la asignatura y por correo sólo se enviarán enlaces a la plataforma.

El objetivo de esta medida se trata de evitar la posibilidad de enviar asignaciones erróneas a los alumnos mediante técnicas de *pishing*.

Mitiga: *Ataque 3.1: Configuración y envío de un correo tipo* pishing, Ataque 3.2: *Obtención de acceso al PC o similar del profesor y envío de correo* y *Ataque 3.3: Robo de credenciales del correo del profesor y envío de correo*.

Medida 7: Al principio de curso se indicará la fecha concreta a partir de la cual estará disponible la asignación de tareas, siendo responsabilidad del alumno visitar la plataforma para consultar la asignación.

El objetivo de esta medida es evitar que el desarrollo normal de la asignatura dependa la recepción de correos electrónicos, ya que articular en correos electrónicos mecanismos similares al acuse de recibo del correo ordinario puede resultar bastante complejo de realizar. Por tanto, los correos advirtiendo de modificaciones en la asignación deberán considerarse una mera cortesía del sistema, y no un mecanismo de notificación formal u oficial.

Mitiga: *Ataque 4.1: Negación de haber recibido el correo con la asignación de tareas.*

Medida 8: Siempre que se genere una nueva asignación de tareas, o se modifique una previamente generada, se enviará una copia de dicha asignación al profesor responsable de la asignatura.

El objetivo de esta medida es que, en caso de que el sistema quede inaccesible por cualquier circunstancia, el profesor de la asignatura pueda disponer de una copia de la asignación de tareas que consultar sin necesidad de acceder al sistema, y que pueda enviar a los alumnos por otros medios.

Mitiga: *Ataque 7.1: Caída del servidor del servidor del sistema (moodle), Ataque 7.2: Caída de las redes de comunicación, Ataque 7.3: Saturación del servidor de Moodle* y *Ataque 7.4: Saturación de las redes de comunicación.*

Medida 9: Realizar una copia de seguridad de la asignación.

El objetivo de esta medida es la de disponer de una copia de los datos de la asignación en caso de fallo, *hardware o software*, del soporte físico donde se aloja.

Mitiga: *Ataque 1.5 Fallo del soporte físico donde se aloja la asignación.*

Premisas de Confianzas	*Medida 1: Mensaje de alerta.* Premisa 1.1. El profesor lee el mensaje de alerta. Premisa 1.2. El profesor entiende el mensaje de alerta. *Medida 2: Resaltar modificaciones.* Premisa 2.1. El usuario revisa las modificaciones. *Medida 3: Solicitar credenciales.* Premisa 3.1. Las credenciales sólo las conoce el profesor. Premisa 3.2. Las credenciales no son fácilmente adivinables por terceros. Premisa 3.3. Las credenciales no son fácilmente generables por pulsaciones aleatorias. *Medida 4: Guardar historial de versiones.* Premisa 4.1. Existe una copia de cada asignación que se desee recuperar. Premisa 4.2. Las versiones están disponibles cuando se requiere su utilización. *Medida 5: Enviar correo para informar de modificaciones.* Premisa 5.1. El correo llega a su destinatario. Premisa 5.2. El destinatario lee su correo. Medida 6: Enviar sólo enlaces por correo. Premisa 6.1. No es factible crear enlaces a servidores externos que puedan suplantar el sistema. Medida 7: Plataforma como único medio de notificación oficial. Premisa 7.1. No es factible suplantar la identidad de la plataforma. Medida 8: Enviar copia de la asignación al profesor. Premisa 8.1. La copia llega a su destinario. Premisa 8.2. El profesor conserva aún la copia en el momento que la necesite. Premisa 8.3. La copia es legible y puede utilizarse cuando se necesite. Premisa 8.4. La copia es adecuada para su utilización a través de otros medios. Medida 9: Copia de Seguridad Al entender que la copia de seguridad se realiza de todo el sistema y no sólo de la asignación de tareas, estas premisas deben estar contenidas dentro del análisis de la seguridad del activo *sistema.*

Contra Argumentos	**Premisa 1.1. El profesor lee el mensaje de alerta.** *Contrargumento 1.1.1 El profesor acepta la eliminación o modificación de la asignación de tareas sin leerla.* Dado que el profesor tiene que introducir además las credenciales para poder llevar a cabo la modificación o eliminación de la asignación, se considera que hay señales de alerta suficientes como para que la responsabilidad de la acción sea suya, no pudiendo culpar de ella a un mal diseño del sistema. Además, si se implementa un historial de versiones, siempre podrá deshacer la acción no deseada restaurando una versión antigua. Por tanto, se asume este riesgo y no se refina más. **Premisa 1.2. El profesor entiende el mensaje de alerta.** *Contrargumento 1.2.1 El profesor acepta la eliminación o modificación de la asignación de tareas sin llegar a entender el mensaje.* Dado que el mensaje no tiene información compleja que mostrar, es de esperar que cualquier usuario pueda entenderlo si lo lee con atención y está escrito con claridad y precisión, como es de presuponer que se haga en un sistema software correctamente desarrollado. Por tanto, este riesgo se considera muy improbable y no se refina más. **Premisa 2.1. El usuario revisa las modificaciones.** *Contrargumento 2.1.1 El profesor acepta la eliminación o modificación de la asignación de tareas sin revisar las modificaciones.* Se entiende que es deber del profesor revisar las modificaciones antes de aceptarlas, por lo que si no lo hace la responsabilidad de la acción será suya, no pudiendo culpar de ella a un mal diseño del sistema. Además, si se implementa un historial de versiones, siempre podrá deshacer la acción no deseada restaurando una versión antigua. Por tanto, se asume este riesgo y no se refina más. **Premisa 3.1. Las credenciales sólo las conoce el profesor.** *Contrargumento 3.1.1. Las credenciales son conocidas por un tercero. Por ejemplo, porque el profesor las tiene apuntadas en una nota adhesiva adherida a su computadora portátil.* Se entiende que es deber del profesor mantener las credenciales de acceso al sistema secretas. Éstas y otras cuestiones sobre las credenciales deberán estar incluidas en el análisis de la seguridad de este activo, por lo que no se refina más. Además, existen mecanismos, como la notificación por medio de correo electrónico y el historial de versiones, que permitirían restaurar la asignación con cierta prontitud en caso de que ésta haya sido modificada de manera no autorizada.

Premisa 3.2. Las credenciales no son fácilmente adivinables por terceros.

Contrargumento 3.2.1. El profesor utiliza como credencial datos que pueden ser conocidos o averiguados por terceros, como el nombre de su mujer, hijos o hijas.

Se entiende que es deber del profesor utilizar credenciales con una fortaleza suficiente para que no puedan ser fácilmente averiguadas por terceros. Éstas y otras cuestiones sobre las credenciales deberán estar incluidas en el análisis de la seguridad de este activo, por lo que no se refina más. Además, existen mecanismos, como la notificación por medio de correo electrónico y el historial de versiones, que permitirían restaurar la asignación con cierta prontitud en caso de que ésta haya sido modificada de manera no autorizada.

Premisa 3.3. Las credenciales no son fácilmente generables por pulsaciones aleatorias.

Contrargumento 3.3.1. El profesor introduce como credencial letras consecutivas del teclado, como "qwert", "1234" o "fghj".
Contrargumento 3.3.2. El profesor introduce como credencial letras repetidas del teclado, como "aaaa", "1111" o "ffgg".

Se considera improbable estos contrargumentos, pero como diseñar nuevas medidas de control para mitigarlos tiene un coste bastante asumible, se diseñan nuevas medidas de control para ellos.

Premisa 4.1. Existe una copia de cada asignación que se desee recuperar.

Contrargumento 4.1.1. La copia que deseamos recuperar no se encuentra en el historial de versiones.

Dado que las asignaciones consumen poco espacio de memoria y no se espera que se modifiquen mucho durante el curso, siempre que se modifica una asignación, se añade una nueva copia de la asignación modificada en el historial de versiones. Por otro lado, estas versiones no se eliminan nunca del historial, por lo que se considera que este contrargumento no podría darse, y no se refina más.

Premisa 4.2. Las versiones están disponibles cuando se requiere su utilización.

Contrargumento 4.2.1. La copia que deseamos recuperar no se encuentra accesible, por fallo del servidor o del soporte donde se almacena.

Dado que el historial de versiones se almacenará con el resto de sistema, su disponibilidad será la misma que la del sistema, y se beneficiará de todas las medidas que se tomen para proteger la disponibilidad del sistema. Por tanto, no se considera necesario refinar este contrargumento más.

Premisa 5.1. El correo llega a su destinatario.

Contrargumento 5.1.1. El sistema de envío de correos falla.

Se añaden nuevas medidas de control para este contrargumento, ya que no es improbable que un sistema de correo falle.

Premisa 5.2. El destinatario lee el correo.

Contrargumento 5.2.1. El profesor proporciona una cuenta de correo que no lee.

Dado que el sistema utilizará el mismo correo que el que el profesor haya proporcionada a la plataforma Moodle, se entiende que el profesor consulta esa dirección de correo con frecuencia, al menos durante el periodo lectivo. En caso de que no lo haya hecho así, se entiende que es responsabilidad de profesor y no podría culpar de ello al sistema. Por tanto, no se refina más este contrargumento.

Contrargumento 5.2.2. El sistema de correos del profesor clasifica el correo de la plataforma como spam.

Dado que el sistema utilizará el mismo correo que el que el profesor haya proporcionado a la plataforma Moodle, se espera que el profesor se haya asegurado de que los correos de Moodle no vayan a su carpeta de *spam*. Por tanto, no se refina más este contrargumento.

Contrargumento 5.2.2. El profesor borra el sistema sin leerlo.

Dado que el sistema trata de evitar explícitamente el envío de correos frecuentes al profesor, estos correos serían ocasionales, por lo que no habría razón para considerarlos rutinarios y borrarlos sin leerlos o prestarles atención. Además, en caso de hacerlo, se entiende que la responsabilidad última de la acción es del profesor y no podría culpar de ella al sistema, por lo que este contrargumento no se refina más.

Premisa 6.1. No es factible crear enlaces a servidores que puedan suplantar el sistema.
Premisa 7.1. No es factible suplantar la identidad de la plataforma.

Ambas cuestiones deberán estar contenidas en el análisis de la seguridad del activo *sistema*, por lo que no se refinan más para este activo.

Premisa 8.1. La copia llega a su destinario.

Contrargumento 8.1.1. El sistema de envío de correos falla.

Se añaden nuevas medidas de control para este contrargumento, ya que no es improbable que un sistema de correo falle.

Contrargumento 8.1.2. El profesor proporciona una cuenta de correo errónea.

Dado que el sistema utilizará el mismo correo que el que el profesor haya proporcionado a la plataforma Moodle, se entiende que la dirección de correo es correcta. Por tanto, no se refina más este contrargumento.

Contrargumento 8.1.3. El sistema de correos del profesor clasifica el correo de la plataforma como spam.

Dado que el sistema utilizará el mismo correo que el que el profesor haya proporcionado a la plataforma Moodle, se espera que el profesor se haya asegurado de que los correos de Moodle no vayan a su carpeta de *spam*. Por tanto, no se refina más este contrargumento.

Premisa 8.2. El profesor conserva aún la copia de la asignación cuando la necesite.

Contrargumento 8.2.1. El profesor ha borrado o perdido la copia de la asignación.

Una vez entregada la copia de la asignación al profesor, su custodia es responsabilidad del profesor y el sistema poco puede hacer por ello. Por tanto, este contrargumento no se refina más.

Premisa 8.3. La copia es legible y puede utilizarse cuando se necesite.

Contrargumento 8.3.1. La asignación no puede leerse por algún fallo de tipo lógico o físico en el soporte de almacenamiento utilizado por el profesor.

Una vez entregada la copia de la asignación al profesor, su custodia es responsabilidad del profesor y el sistema poco puede hacer por ello. Además, la probabilidad de que falle el servidor del sistema o las redes de comunicaciones a la vez que el soporte de almacenamiento del profesor se considera muy baja, por lo que este contrargumento no se refina más.

Premisa 8.4. La copia es adecuada para su utilización a través de otros medios.

Contrargumento 8.4.1. La copia pesa mucho y no se puede enviar fácilmente por sistemas como correo, foros o whatsapp.

Se añaden nuevas medidas de control para este contrargumento, ya que su realización tiene un coste asumible.

Contrargumento 8.4.2. La copia tiene un formato no aceptado por los medios alternativos a utilizar.

Se añaden nuevas medidas de control para este contrargumento, ya que su realización tiene un coste asumible.

Medidas de Control (2)	**Medida 10: Se deberá chequear que las credenciales del profesor no estén compuestas en su mayoría por letras adyacentes un teclado estándar o letras repetidas.** El objetivo de esta medida es evitar que se pueda generar las credenciales del profesor por pulsaciones aleatorias en un teclado como consecuencia de que el profesor haya guardo un dispositivo sin bloquear en el bolsillo de un pantalón o en una maleta. Mitiga: *Contrargumento 3.3.1 (letras consecutivas)* y *contrargumento 3.3.2 (letras repetidas).* **Medida 11. Si fallase el envío de un correo al profesor responsable de la asignatura para notificarlo de la modificación o eliminación de la asignación, se notificará de este hecho al profesor la próxima vez que acceda al sistema.** El objetivo de esta medida es buscar una manera alternativa de informar al profesor de los cambios realizados en la asignación ante la imposibilidad de hacerlo vía correo electrónico. Mitiga: *Contrargumento 5.5.1 (fallo sistema de correo)* y *contrargumento 8.8.1 (fallo sistema de correo).* **Medida 12. La copia de la asignación enviada al profesor deberá estar en formato pdf y tener un tamaño en bytes lo más reducido posible.** El objetivo es que la asignación pueda enviarse con facilidad por sistemas auxiliares. Para ello, conviene que el archivo pese lo menos posible y tenga un formato lo más estándar posible. Mitiga: *Contrargumento 8.4.1 (peso)* y *Contrargumento 8.4.2 (compatibilidad).*
Premisas de Confianzas (2)	*Medida 10: Caracteres no consecutivos* Premisa 10.1. Sólo se pueden adivinar con facilidad por pulsación aleatoria contraseñas con caracteres adyacentes en el teclado o repetidos. Premisa 10.2. El usuario utiliza un teclado tipo qwerty. *Medida 11: Aviso de modificación vía plataforma.* Premisa 11.1 Se consigue registrar la notificación en la plataforma. Premisa 11.2 El profesor accede al sistema con una frecuencia suficiente como para que el cambio efectuado no esté visible un periodo excesivo de tiempo, de manera que pueda ser visualizado por un amplio número de alumnos y afectar de manera no desdeñable al desarrollo de la asignatura.

	Medida 12. PDF Ligero Premisa 12.1: Los sistemas auxiliares permiten el envío de archivos. Premisa 12.2: Los sistemas auxiliares permiten el envío de archivos pdfs. Ambas premisas son perfectamente asumibles por los sistemas de hoy en día, por lo que no se refinan más.
Contra Argumentos (2)	**Premisa 10.1. Sólo se pueden adivinar con facilidad por pulsación aleatoria contraseñas con caracteres adyacentes en el teclado o repetidos.** *Contrargumento 10.1.1. Existen otras combinaciones de teclas con probabilidad de generar credenciales por pulsaciones aleatorias.* Como de momento no se conocen esas combinaciones de teclas, no se refina más este contrargumento. **Premisa 10.2. El usuario utiliza un teclado tipo *qwerty*.** *Contrargumento 10.2.1. El usuario utiliza un teclado no qwerty.* Los teclados no qwerty, aunque existentes, son muy inusuales, por lo que se asume el riesgo y no se refina más este contrargumento. **Premisa 11.1 Se consigue registrar la notificación en la plataforma.** *Contrargumento 11.1.1. La base de datos se cae justo antes de registrar la notificación.* En este caso, la base de datos habría estado operativa durante el desarrollo de la modificación o eliminación de la asignación, tendría que fallar el sistema de correos, y luego caerse además la base de datos una vez guardada la asignación. Dado que la probabilidad de que estos tres sucesos ocurran a la vez es muy baja, se asume el riesgo y no se refina más este contrargumento. **Premisa 11.2 El profesor accede al sistema con frecuencia.** *Contrargumento 11.1.1. La modificación y eliminación de la asignación se realiza justo al inicio de un periodo festivo largo, como un puente o las navidades, por lo que el profesor no accede al sistema durante todo ese periodo, pero diversos alumnos sí acceden para consultar qué tareas tenían asignadas y prepararlas.*
Comentarios	(1) Se ha considerado la posibilidad de firmar digitalmente todos los correos electrónicos enviados por el profesor, tanto de manera personal como desde la plataforma. No obstante, como la gestión de firmas digitales no tiene aún suficiente implantación dentro del mundo académico, se ha descartado por el momento esta posibilidad.