

# Estudio 4



Estudio de seguridad  
de la plataforma.



# Índice

---

Consideraciones previas.....	2
Acceso seguro a la plataforma de telemedicina. ....	3
Disposiciones generales. ....	6
Documento de Seguridad.....	7
Privacidad de la Sala Virtual. ....	11
Conclusiones .....	13
Referencias.....	14

CONTROL DE VERSIONES			
Revisión	Autor	Fecha	Motivo
1	José Criado SICBRAIN EUROPA SL	27/12/2011	Primera versión del Estudio 4.

## Estudio 4. Estudio de seguridad de la plataforma.

---

El siguiente estudio tiene como finalidad la identificación de los estándares que la plataforma RESATER debe cumplir, tal y como expone el oferente realizado por SICBRAIN EUROPA SL para esta propuesta, realizando un seguimiento y autoevaluación de las medidas que se han ido desarrollando para asegurar la confiabilidad de este “canal de comunicación”. Para ello se evaluará el sistema de permisos ACL (Access Control List) utilizado en la implementación de la plataforma, se identificarán posibles casos de acceso y se realizará una normativa de prevención y seguridad acorde con la utilización que los usuarios profesionales van realizar dentro de este entorno de transferencia de conocimientos internacional.

### *Consideraciones previas.*

---

Tal y como se expuso en el Estudio 1 titulado “Estudio de factibilidad, adaptación de las aplicaciones y servicios a la plataforma”, en el apartado *Análisis de seguridad asociada a la Plataforma de Telemedicina*, en un primer momento se estimó la posibilidad de implementar un algoritmo criptográfico RSA. Este método permitía dotar a la plataforma de una seguridad y robustez muy elevada, pero se descartó puesto que para el espacio de colaboración que engloba el consorcio RESATER las medidas adoptadas eran excesivas, sufriendo con ello penalizaciones para la usabilidad del día a día por parte de los profesionales, y disminuyendo por tanto el rendimiento esperado. El carácter práctico de esta propuesta reside en un entorno fiable y seguro, y la no inclusión de este algoritmo supone aumentar la productividad de los recursos asociados.

Otro de los aspectos citados en dicho estudio fue la gestión de los riesgos asociados. “La protección de la plataforma ha de ser proporcionada a los riesgos”. Esta frase resume la implementación que se ha desarrollado para la elaboración de los permisos de acceso y la dimensión de las categorías asignadas, según el rol de entrada a la plataforma. Una correcta gestión de la misma permitirá aumentar la confiabilidad otorgada por el cumplimiento de las normativas europeas en relación con la protección de datos y la gestión de archivos y ficheros asociados a una base de datos de las características de la plataforma RESATER.

El estudio jurídico realizado para esta plataforma concluye que las principales leyes que rigen este tipo de tratamiento son:

- Ley Orgánica 15/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal (LOPDGP). - España
- Ley Nº 78-17, de 6 de enero de 1978, relativa a la informática, los ficheros y las libertades. - Francia
- Ley Nº41 de 18 de Agosto (Tratamiento de datos personales y la protección de la privacidad en las Comunicaciones Electrónicas). - Portugal

El desarrollo software realizado cumple con dicha normativa asegurando en todo momento la confiabilidad y privacidad de los datos almacenados, siguiendo una serie de medidas de cara al usuario final que se desarrollarán más adelante.

### ***Acceso seguro a la plataforma de telemedicina.***

Para la validación de los usuarios del consorcio RESATER (y los diferentes roles expuestos) se ha desarrollado un sistema de control de acceso a través de un *framework* de lenguaje PHP denominado CakePHP. Las características principales de este entorno de desarrollo son las siguientes:



Compatible con PHP4 y PHP5	CRUD integrado para la interacción con BBDD
Soporte de aplicación (scaffolding)	Arquitectura Modelo Vista Controlador (MVC)
Validación integrada	Componentes de email, cookie, seguridad, sesión y manejo de solicitudes
Listas de control de acceso flexibles	Caché flexible
Despachador de peticiones (dispatcher)	Localización

**Figura 1.** Características principales del framework CakePHP

El sistema de acceso a la plataforma se ha desarrollado orientado a los profesionales del consorcio RESATER. Es por ello que para acceder a las entidades y/o centros hay que realizar una primera validación como profesional asociado a la plataforma.

Uno de los aspectos clave de la seguridad implantada es la separación que realiza la lógica del funcionamiento del sistema de la relativa a la capa de aplicación, es decir, se manejarán por separado los usuarios y los profesionales en la base de datos.

### Creación de un usuario asociado.

El establecimiento del perfil profesional lleva consigo agregado la creación automática de un usuario asociado. Los pasos que se realizan son los siguientes:

1. Verificación del nombre de usuario. Se comprueba que sea único dentro del sistema.
2. Asignación de la primera contraseña: será el correo electrónico suministrado.
3. Generación de un campo codificado para validar la cuenta.
4. Cuando un usuario ha sido creado, recibe en su email un correo electrónico con el campo codificado indicando el procedimiento para validar la cuenta. Los datos recibidos son los siguientes:
  - a. Nombre de usuario.
  - b. Contraseña (inicialmente el correo electrónico suministrado).
  - c. Cadena de validación de cuenta (cifrada).
5. Confirmación de cuenta: una vez que el usuario ingresa en el sistema (con su nombre de usuario y contraseña inicial) se le redirige a una ventana de confirmación de cuenta. En ella deberá introducir la cadena de validación recibida en el email inicial.
6. Requerimiento de cambio de contraseña: otra de las medidas que refuerzan la seguridad de este sistema de acceso será el requerimiento obligatorio del cambio de contraseña.

7. Validación final: una vez que el cambio de contraseña se realizó correctamente (la cadena de validación coincide con la generada en la creación de la cuenta), el usuario pasa a estar activo y asociado a un profesional, por lo que puede acceder a la información y los servicios expuestos.

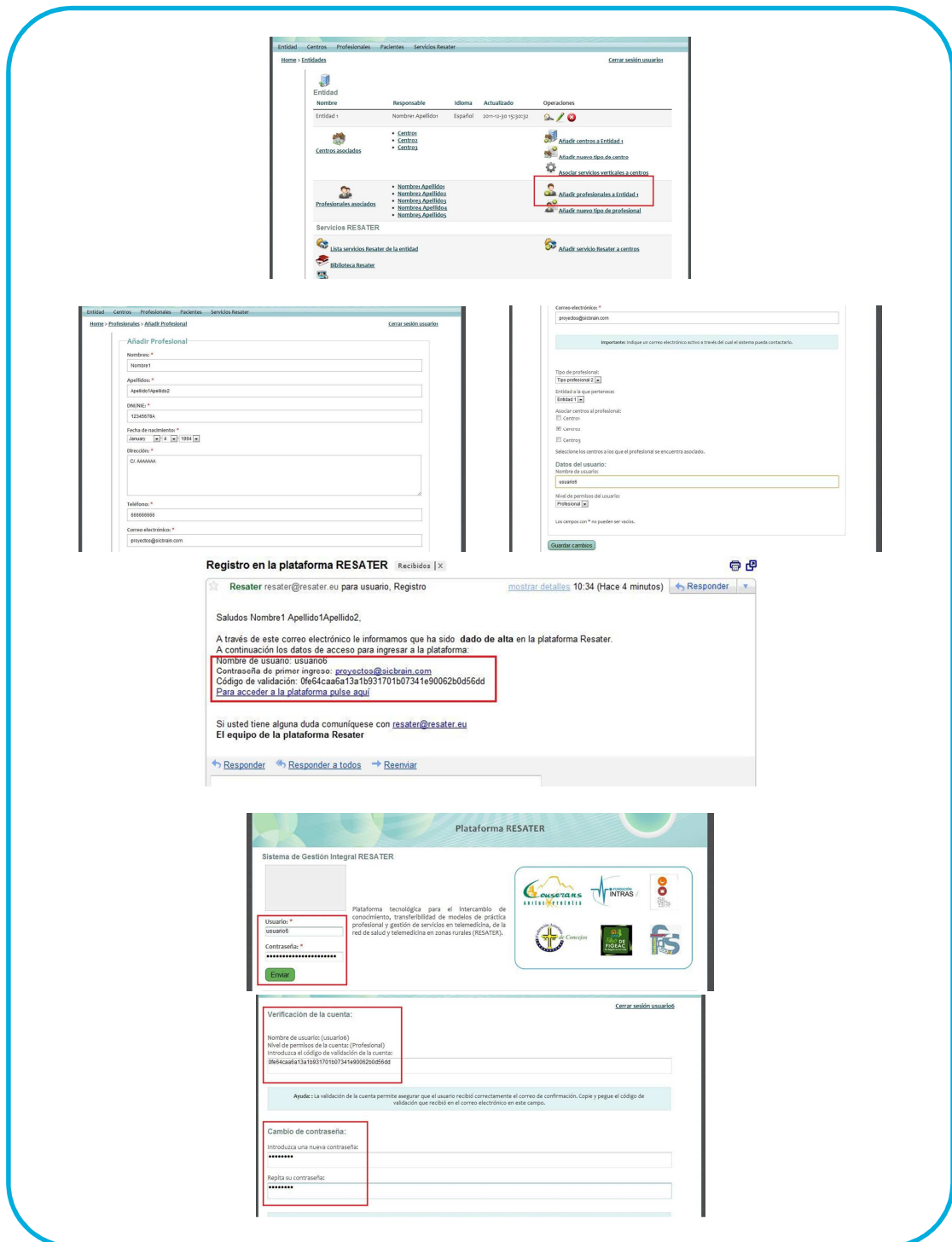


Figura 2. Proceso de creación de un usuario asociado

La codificación realizada para la creación de contraseñas de usuario se realiza a través de un *hash* propio que CakePHP utiliza. Será una cadena de información privada la que se utilice para esta compresión, sin usar con ello métodos clásicos como base64 ó encode/decode. Este sistema permite dotar a la plataforma de un excelente nivel de seguridad y confiabilidad a la hora de crear nuevos usuarios que puedan por tanto acceder a la información contenida dentro de los módulos existentes.

El sistema de permisos utilizado para las funciones de los diferentes servicios de la plataforma entre los ACOs y AROs creados se denomina ACL (cuando un ARO puede acceder a un ACO). ACO (Access Control Object) es el objeto que se quiere controlar, y ARO (Access Request Object) es el objeto que solicita el control de algo. Este sistema estructura los usuarios en grupos, y una vez organizados, se indica qué acciones puede ejecutar cada grupo. La seguridad implícita permite que cuando un usuario no dispone de los privilegios suficientes para realizar una operación, el sistema no le permite acceder a ella. Esta gestión de permisos garantiza por tanto la seguridad en cuanto al acceso de usuarios se refiere según las restricciones definidas en el diseño y la legislación existente relativa a la privacidad de los datos.

### ***Disposiciones generales.***

---

Dentro de este Estudio 4 se abarca, entre otros aspectos, el reglamento que especificará las medidas de carácter técnico y organizativo necesarias que garanticen la seguridad de los ficheros compartidos entre los profesionales del consorcio RESATER, así como las bases de datos generadas.

Las medidas de **“carácter básico”** abordan los ficheros que contienen los datos de carácter personal. Es decir, todos aquellos campos registrados por los profesionales, entidades y centros recogidos de los correspondientes formularios. Éstos serán almacenados dentro del servidor Linux de la plataforma, provisto de sus correspondientes medidas de seguridad que permiten garantizar la confiabilidad de los mismos. Será decisión del consorcio RESATER el nombrar a uno o varios responsables de dicha información.

Las medidas de **“nivel medio”** contienen una mayor repercusión, pues abarcan información financiera o administrativa que permita evaluar a los profesionales en términos de “situación personal”, y como es lógico este no es el cometido de la plataforma. Su uso se

restringe, en un primer momento, al intercambio de información y al espacio colaborativo creado a través de la Sala Virtual, y las diferentes herramientas habilitadas de chat y transferencia de ficheros.

Un tercer grupo de medidas, las denominadas de “**nivel alto**”, no serán aplicables a esta plataforma, tal y como se expuso en el Estudio 1, hoja 11, pues no se contemplan en el ámbito al que está destinada la plataforma de telemedicina.

La conclusión obtenida este tipo de disposiciones es que el propio consorcio RESATER nombre a los responsables para este tipo de información, asegurando SICBRAIN EUROPA SL el traspaso de información de una forma clara y explícita, respondiendo en todo momento por el almacenamiento de datos realizado y el soporte software que lo maneja.

### ***Documento de Seguridad.***

---

Un documento de seguridad es una herramienta evaluadora que permite informar a cualquiera de las personas autorizadas que así lo considere sobre el mantenimiento de la seguridad asociada a la plataforma de telemedicina. Concretamente el responsable de los ficheros y carpetas, en función de una normativa interna, debe anotar cualquier modificación relevante que se considere. Este tipo de incidencias debe cumplir en todo momento la legislación europea que concierne a la protección de datos, garantizando en todo momento la privacidad de los mismos. Como referencia se tomarán las consideraciones de la **Agencia Española de Protección de Datos**, puesto que sus normativas al respecto se consideran de ámbito general y aplicable al resto de leyes de los estados francés y portugués.

## **DOCUMENTO DE SEGURIDAD**

### **CAPÍTULO 1: ÁMBITO DE APLICACIÓN.**

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad del consorcio RESATER.

Las medidas de seguridad se califican en tres niveles acumulativos (básico, medio y alto) atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.



## CAPÍTULO 2: MEDIDAS, NORMAS Y PROCEDIMIENTOS ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS.

Identificación y autenticación: Medidas y normas relativas a la identificación y autenticación de los profesionales del consorcio RESATER autorizados al acceso a la plataforma.

- × Identificación de los usuarios de forma inequívoca y personalizada, verificando su autorización. Al realizarse mediante contraseña, se garantiza la confidencialidad e integridad, recomendando su cambio en una periodicidad no superior a un año.

Control de acceso: El sistema de alta de un nuevo usuario incluye una primera validación, previa inserción de una “cadena de validación de cuenta” que ha recibido en su email personal.

Los usuarios accederán a aquellos datos y recursos que precisen para el desarrollo de sus funciones. El responsable del fichero establecerá mecanismos para evitar que un usuario de la plataforma RESATER pueda acceder a recursos con derechos distintos de los autorizados.

Exclusivamente el súper-administrador podrá conceder, alterar o anular el acceso autorizado, velando en todo momento por la seguridad de la plataforma y la gestión de recursos disponibles en la misma.

Registro de accesos: Salvo petición expresa del consorcio RESATER, no se almacenará la identificación del usuario, la fecha y hora, y el fichero accedido o tipo de acceso realizado.

Gestión de soportes y documentos: Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen y ser inventariados; serán almacenados en el servidor Linux, lugar de acceso restringido al que sólo tendrá acceso el personal que se encuentre habilitado para tal efecto, dependiendo siempre del súper-administrador.

Copias de seguridad: Se realizarán copias de seguridad con una periodicidad diaria, pudiéndose restaurar de forma inmediata (con un margen de dos horas) los datos con una

antelación de 7 días. Contendrá tanto los ficheros almacenados como las bases de datos que subyacen bajo el software de la capa de usuario de la plataforma RESATER. Los procedimientos establecidos para las copias de respaldo garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción, así como cualquier versión de la copia de seguridad que se desee de los 7 días anteriores.

Responsable de seguridad: Se designará a un responsable de seguridad dentro del consorcio RESATER, o en su caso, el súper-administrador del sistema, que con carácter general se encargará de coordinar y controlar las medidas definidas en este documento de seguridad.

### **CAPÍTULO 3: PROCEDIMIENTO GENERAL DE INFORMACIÓN A LOS USUARIOS.**

Para asegurar que todos los usuarios conocen las normas de seguridad que afectan al desarrollo de sus funciones, este documento podrá ser visible o difundido a través de la propia plataforma RESATER o del Observatorio creado para tal efecto.

### **CAPÍTULO 4: FUNCIONES Y OBLIGACIONES DE LOS USUARIOS.**

Todos los usuarios que accedan a la plataforma del consorcio RESATER están obligados a conocer y observar las medidas, normas y procedimientos que afecten a las funciones que desarrolla.

Todos los usuarios deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

### **CAPÍTULO 5: PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS.**

Se considerarán como “incidencias de seguridad”, entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal de los profesionales asociados al consorcio RESATER.

### **CAPÍTULO 6: PROCEDIMIENTOS DE REVISIÓN.**

El Documento de Seguridad será revisado por el responsable de seguridad designado con una periodicidad no superior a los 30 días, estableciendo con ello una hoja de control “manual” que sirva de evaluación de los registros e incidencias ocasionados, estando en todo momento actualizado. De hecho, deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los ficheros o como consecuencia de los controles periódicos realizados.

**Tabla 1.** Documento de seguridad – Normativa.

Las hojas a cumplimentar deberán presentar el siguiente formato. En él se detallará el tipo de incidencia (en el caso de que fuese una revisión periódica, rellenar la correspondiente casilla con “notificación periódica”), el número de la revisión, el tipo de usuario que tuvo la incidencia (para identificar el rol de acceso a la plataforma) y su nombre, así como la fecha de la incidencia y el motivo causante de la revisión realizada, de una forma más extensa que en el título inicial.

Tipo de Incidencia:				
Revisión	Tipo de usuario	Nombre	Fecha	Motivo

**Tabla 2.** Informe de seguridad (para cumplimentar)

Con este seguimiento sobre las incidencias y los profesionales que acceden a la plataforma del consorcio RESATER se tendrá una constante evaluación del rendimiento y usabilidad que proporciona a todos esta plataforma.

Así mismo el responsable de seguridad elaborará un listado de los usuarios (con sus diferentes tipos de permisos) que se actualizará con cualquier cambio o novedad que repercuta en la lista de personas que tienen acceso a la plataforma.

### ***Privacidad de la Sala Virtual.***

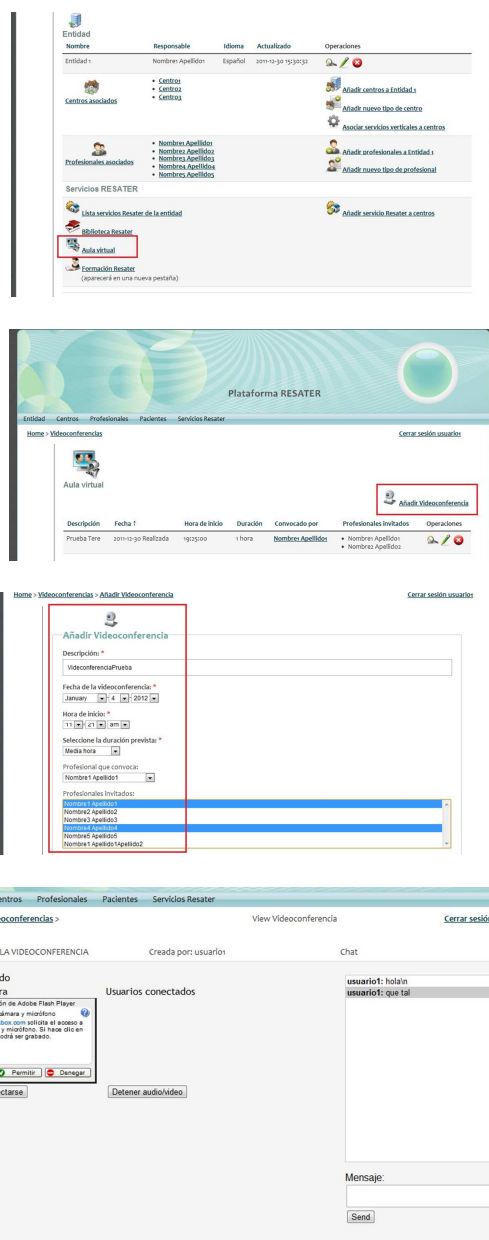
---

La sala virtual de la plataforma RESATER es uno de los módulos de los que consta dicha plataforma de profesionales. En ella se podrán establecer videoconferencias y chat para así permitir participar a todos los usuarios dentro de este espacio de colaboración internacional, consiguiendo así la interoperabilidad entre profesionales para una mejor prestación de sus servicios asociados.

La privacidad que posee esta sala se encuentra en consonancia con el resto de medidas de seguridad adoptadas en el entorno de la plataforma de los profesionales. El funcionamiento de la misma es el siguiente:

1. Los profesionales asociados a la plataforma podrán establecer una videoconferencia y enviar invitaciones tanto a otros profesionales que tengan su propio login y password para acceder a la plataforma, como a profesionales externos a los que la url de validación de acceso les llegará por correo electrónico.
2. Una vez enviadas las invitaciones para una sesión de videoconferencia concreta, los profesionales internos podrán observar dicha invitación en su “vista de videoconferencias”, y acceder a la misma una vez activada.
3. La seguridad de este sistema restringe al creador de la videoconferencia como el primer profesional que accede a la misma. El resto de usuarios invitados tendrán acceso una vez se haya realizado esta validación. Internamente el sistema posee tres niveles de acceso para comprobar los permisos de cada usuario al respecto.
4. Cuando un usuario invitado accede, se comprueba (en un nivel inferior) con un “token” que dicho invitado se encuentra en la base de datos de esa videoconferencia. En el caso de no haber dado comienzo la misma, le aparecerá un mensaje que le indica este estado.
5. Si un “intruso” consigue acceder a la url donde se establecerá la videoconferencia, pero no ha sido invitado por el creador, se le mostrará por pantalla la no inclusión

en la base de datos de la misma, denegándole el correspondiente acceso. Este tipo de protección completa la seguridad para que no se pueda hacer un uso malintencionado del acceso a una sesión dentro de la sala virtual.



**Figura 3.** Acceso a una videoconferencia del módulo Sala Virtual

## Conclusiones

---

La seguridad asociada a la plataforma de telemedicina del consorcio RESATER es uno de los aspectos clave para la correcta implementación de la misma. El cumplimiento de la legislación europea en materia de sistemas de comunicación online y tratamiento de datos personales regula dichas áreas con una gran disciplina dentro de dicho marco jurídico, en referencia a los países de España, Francia y Portugal. Es por ello que todos los accesos a bases de datos e información “sensible” se rige por la limitación y el control de los usuarios registrados y la permisología asociada a cada uno de ellos.

El sistema de acceso a la plataforma se validará, en un primer establecimiento, a través de una “cadena de validación de cuenta” recibida en el propio email, confirmando posteriormente la incorporación de un nuevo usuario a la base de datos del sistema. Este proceso de seguridad se ha desarrollado a través de un *hash* propio del entorno de desarrollo CakePHP, consiguiendo con ello una gran confiabilidad en la seguridad implícita que el software de la plataforma posee. El sistema de permisos utilizado para ello se denomina ACL, y pone en relación a ACOs y AROs creados, que estructuran los usuarios en diferentes grupos, cada uno de ellos con un conjunto de privilegios determinado.

En cuanto a las medidas de carácter técnico y organizativo existentes, en relación con la seguridad de los ficheros compartidos y las bases de datos creadas, se han contemplado tres tipos de niveles: bajo, medio y alto. El primero de ellos considera los datos de carácter personal, registrados a través de los formularios iniciales de recogida de datos. El nivel medio se centra en la identificación personal del usuario a través de la información almacenada, estando restringido su acceso a la práctica totalidad de los usuarios. Por último, las medidas de nivel alto no se han contemplado en este espacio de colaboración por tener una naturaleza diferente de la prevista en la descripción del uso y finalidad de la plataforma del consorcio RESATER.

El documento de seguridad (y la normativa que conlleva) pretende identificar una serie de procedimientos para que todos los usuarios y el/los responsable/s de la documentación almacenada cumplan con las directrices establecidas. Son medidas de carácter básico que permiten reforzar la seguridad que el propio software desarrollado garantiza, para así actualizar y mejorar el funcionamiento de la plataforma, siendo con ello un entorno dinámico y altamente escalable ante cualquier cambio que se solicite.

Por último, la privacidad asociada a la Sala Virtual de la plataforma refuerza aún más la imposibilidad de hacer un uso malintencionado de sus recursos, permitiendo acceder a dichas videoconferencias a personas que no se encuentren asociadas al consorcio RESATER (pero que un profesional interno considere que deben estar) en una vista paralela, comprobando en todo momento su acceso a través de las bases de datos creadas que identifican los usuarios invitados a dicha sesión.

### ***Referencias***

---

- [1] <http://cakephp.org>
- [2] <http://www.aepd.es>
- [3] <http://www.tokbox/opentok/>
- [4] Estudio 3. “Estudio jurídico de la plataforma RESATER”