

Estudo 4



Estudo de segurança
da plataforma



Índice

Considerações preliminares.....	2
Garantir o acesso à plataforma de telemedicina.....	3
Disposições gerais.....	6
Documento de segurança.....	7
Privacidade Sala Virtual.....	10
Conclusões.....	13
Referências.....	14

Controle de Versão			
Revisão	Autor	Data	Razão
1	José Criado SICBRAIN EUROPA SL	27/12/2011	Primeira versão do estudo 4.

Estudo 4. Estudo de segurança da plataforma.

O estudo a seguir tem como objetivo identificar as normas que devem atender plataforma RESATER, como exposto pelo ofertante SICBRAIN EUROPA SL para esta proposta, acompanhamento e auto-avaliação têm sido desenvolvidos para garantir a confiabilidade deste "canal de comunicação". Isto irá permitir avaliar o sistema de ACL (Access Control List) utilizados na implementação da plataforma, identificar possíveis casos de acesso e será uma regulamentos de prevenção e segurança de acordo com o uso que os utilizadores profissionais irão realizar nesta ambiente de transferência de conhecimento internacional.

Considerações preliminares.

Como discutido no Estudo 1, intitulado "Estudo de viabilidade, a adaptação de aplicações e plataforma de serviços", na seção Verificação de segurança associados com a Plataforma de Telemedicina, em primeiro lugar estimada a possibilidade de implementação de um algoritmo de criptografia RSA. Este método permitiu a plataforma para fornecer uma segurança muito elevada e robustez, mas foi descartada uma vez que para o espaço de colaboração que abrange a RESATER consórcio as medidas tomadas eram excessivos, assim, sofrer penalidades para a usabilidade da vida cotidiana por profissionais e, assim, diminuindo o retorno esperado. A praticidade da proposta reside em um ambiente confiável e seguro, bem como a exclusão deste algoritmo envolve o aumento da produtividade dos recursos associados.

Outro aspecto mencionado neste estudo foi a gestão de riscos. "A proteção da plataforma devem ser proporcionais aos riscos." Esta frase resume a implementação que foi desenvolvido para a preparação de permissões de acesso eo tamanho das categorias atribuídas, dependendo da função de entrada para a plataforma. Gestão adequada de que vai aumentar a confiabilidade conferida pela conformidade com as normas europeias de protecção de dados e gerenciamento de arquivos e arquivos associados a um banco de dados de recursos da plataforma RESATER.

A empresa realizou para esta plataforma conclui que as principais leis que regem este tipo de tratamento são:

- Lei 15/1999 de 13 de Dezembro, de Protecção de Dados Pessoais (LOPDGP). - Espanha

- Lei n.º 78-17 de 06 de janeiro de 1978 em informática, arquivos e liberdades. - França

- Lei n.º 41 de 18 de Agosto (Tratamento de dados pessoais e protecção da privacidade nas comunicações electrónicas). - Portugal

O desenvolvimento de software feito em conformidade com tais regras em todos os momentos garantir a confiabilidade e privacidade dos dados armazenados, após uma série de passos para o usuário final que será desenvolvido mais tarde.

Garantir o acesso à plataforma de telemedicina.

Para validar os usuários consórcio RESATER (e os diferentes papéis expostos) desenvolveu um sistema de controle de acesso através de uma conhecida PHP framework CakePHP. As principais características deste ambiente de desenvolvimento são:



Compatível com PHP4 e PHP5	CRUD integrado para interação com DB
Suporte de aplicação (scaffolding)	Architecture Model View Controller (MVC)
Validação integrada	Componentes de e-mail, cookie, a segurança da sessão, e gerenciamento de aplicativos.
Listas de Controle de Acesso flexível	Cache flexível
Pedidos Dispatcher (dispatcher)	Localização

Figura 1. Principais características do quadro CakePHP

O sistema de acesso foi desenvolvido plataforma destinada a profissionais de consórcio RESATER. É por isso que o acesso às entidades e / ou centros devem realizar uma primeira validação como um profissional associado com a plataforma.

Um dos aspectos-chave das práticas de segurança é a separação que executa a operação lógica do sistema sobre a camada de aplicação, ou seja, serão tratados separadamente e usuários profissionais no banco de dados.

Criando um usuário associado.

O estabelecimento do perfil profissional traz adicionado a criação automática de um usuário associado. As etapas executadas são:

1. Verificando nome de usuário. Verifica-se que é único dentro do sistema.
2. Atribuindo a primeira senha: e-mail serão fornecidos.
3. Geração de um campo codificado para validar a conta.
4. Quando um usuário foi criado, receber via e-mail um e-mail com o campo criptografado, indicando o procedimento para validar a conta. Os dados recebidos são os seguintes:
 - a. Nome de Usuário.
 - b. Senha (inicialmente e-mail fornecido).
 - c. Cadeia de validação de conta (criptografada).
5. Confirmação de conta: Quando o usuário entra no sistema (com seu usuário e senha inicial) é redirecionado para uma conta de janela de confirmação. Deve entrar na cadeia de validação recebidos no e-mail inicial.
6. Solicitação de alteração de senha: uma das medidas que melhorem a segurança do sistema de acesso é o requisito obrigatório da mudança de senha.
7. Validação Final: Uma vez que a mudança de senha foi bem sucedida (o processo de validação coincide com a que gerou a criação da conta), o usuário torna-se ativo e associada com um profissional, para que você possa acessar as informações e expostos serviços.

The image displays the user registration process for the RESATER platform, divided into three main sections:

- Top Section: 'Añadir Profesional' Form**
 - Entity Management:** A table with columns: Entidad, Responsable, Idioma, Actualizado, Operaciones. It lists 'Entidad 1' and 'Centros asociados'.
 - Professional Management:** A section for adding professionals, including fields for 'Nombre', 'Apellido', 'ID', 'Fecha de nacimiento', 'Dirección', 'Teléfono', and 'Correo electrónico'.
 - Services Management:** A section for adding services, including fields for 'Tipo de profesional', 'Entidad a la que pertenece', 'Asociar centros al profesional', 'Datos del usuario', and 'Nivel de permisos del usuario'.
- Middle Section: 'Registro' Email**
 - Header:** 'Resater resater@resater.eu para usuario, Registro'.
 - Body:** A message in Spanish stating that the user has been registered and providing login instructions. It includes a red box highlighting the login details: 'Nombre de usuario: usuario', 'Contraseña de primer ingreso: proyector@nicbrain.com', and 'Código de validación: 0fe64caa6a13a1b931701b07341e90062b0d56dd'.
 - Footer:** Contact information for the platform support team.
- Bottom Section: Login and Verification**
 - Login Form:** A form with fields for 'Usuario' and 'Contraseña'.
 - Verification Form:** A form for verifying the account, including fields for 'Nombre de usuario', 'Nivel de permisos de la cuenta', and 'Código de validación'.
 - Password Change Form:** A form for changing the password, including fields for 'Introduzca una nueva contraseña' and 'Repita su contraseña'.

Figura 2. O processo de criação de um usuário associado

A codificação feito para a criação de senhas de usuários é feito através de uma CakePHP próprio hash usa. Ser uma sequência de informação privada que é usada para essa compressão, portanto, sem o uso de métodos tradicionais ou como base64 codificação / decodificação. Este sistema permite que a plataforma para oferecer um excelente nível de

segurança e confiabilidade ao criar novos usuários podem, assim, acessar as informações contidas dentro dos módulos existentes.

O sistema de licenças usadas para as funções dos diversos serviços da plataforma entre os ACOs e AROs criado é chamado ACL (quando um ARO pode ter acesso a um ACO). ACO (Object Access Control) é o objeto a ser controlado, e ARO (Object Request Access) é o objeto que as solicitações de controle de alguma coisa. Estruturas do sistema os usuários em grupos, e uma vez organizado, isto indica que ações você pode executar cada grupo. A segurança implícita significa que quando um usuário não tem privilégios suficientes para executar uma operação, o sistema não permitir o acesso. Esta gestão permite de garantias de segurança de modo a respeitar o acesso do usuário como restrições definidas no projeto e na legislação em vigor sobre a privacidade dos dados.

Disposições gerais.

Neste estudo 4 é composta, entre outras coisas, o regulamento especificará as medidas técnicas e organizativas adequadas para garantir a segurança dos arquivos compartilhados entre os profissionais consórcio RESATER, e as bases de dados gerado.

As medidas de "**caráter básico**" arquivos de endereço que contenha dados pessoais. Ou seja, todos aqueles gravados por áreas profissionais, organizações e centros das formas correspondentes coletados. Estes serão armazenados dentro da plataforma do servidor Linux, equipado com as medidas de segurança correspondentes que garantem a confiabilidade dos mesmos. RESATER decisão do consórcio será a de nomear um ou mais responsáveis por essa informação.

As medidas de "**média**" contêm um impacto maior, pois eles cobrem a informação financeira e administrativa para avaliar os profissionais em termos de "situação pessoal", e obviamente este não é o papel da plataforma. Seu uso é restrito, a princípio, a troca de informações e espaço colaborativo criado através da Sala Virtual e ferramentas diferentes habilitado bate-papo e transferência de arquivos.

Um terceiro grupo de medidas, o chamado "**alto nível**" não se aplica a esta plataforma, como discutido no Estudo 1, página 11, eles não estão cobertos na área da política destina-se plataforma de telemedicina.

A conclusão destas disposições é que o próprio consórcio RESATER nome os responsáveis por este tipo de informação, assegurando EUROPA SL informações transferência

SICBRAIN de forma clara e explícita, armazenamento de dados responder em todos os momentos e feitos software de apoio que o gerencia.

Documento de segurança.

Um documento de segurança é uma ferramenta de avaliação que permite informar qualquer pessoa autorizada a fazê-lo considerar a manutenção da segurança associados com a plataforma de telemedicina. Especificamente responsável por arquivos e pastas, de acordo com os regulamentos internos, você deve anotar todas as mudanças significativas a ser considerado. Estes incidentes devem cumprir a legislação em todos os tempos Europeia relativa à protecção de dados, assegurando a privacidade em todos os momentos do mesmo. Como referência, tomar as considerações da **Agência Espanhola de Protecção de Dados**, como sua política a este respeito são consideradas de âmbito geral e aplicável a outras leis estaduais Francês e Português.

DOCUMENTO DE SEGURANÇA

CAPÍTULO 1: SCOPE.

Este documento se aplica a arquivos contendo dados pessoais são de responsabilidade da RESATER consórcio.

Medidas de segurança são classificados em três níveis cumulativos (elementar, médio e alto) de acordo com a natureza das informações discutidas em relação à necessidade maior ou menor para garantir a confidencialidade e integridade das informações.

CAPÍTULO 2: medidas, normas e procedimentos para garantir os níveis de padrões de segurança.

Identificação e autenticação: Medidas e padrões para a identificação e autenticação dos profissionais RESATER consórcio autorizado o acesso à plataforma.

- × Identificar os usuários exclusivamente personalizado e verificar a sua autorização. Quando realizada por uma senha, garantindo a confidencialidade e integridade, recomendando a mudança de intervalos não superiores a um ano.

Controle de acesso: o sistema em cima de um novo usuário inclui uma primeira validação, mediante inserção de uma "cadeia de validação de conta" que você recebeu no seu e-mail pessoal.

Usuários acesso aos dados e recursos necessários para o desempenho das suas funções. Controladores deve estabelecer mecanismos para impedir que um usuário da plataforma RESATER podem acessar os recursos com outros direitos que não os autorizados.

Apenas o administrador do super-pode conceder, alterar ou cancelar o acesso autorizado, garantindo em todos os momentos para a segurança da plataforma e da gestão dos recursos nele.

Log de acesso: A menos que não pedido específico da RESATER consórcio armazenar o ID do usuário, data e hora, eo tipo de arquivo de acesso permitido ou feito.

Gerenciamento de mídias e documentos: A mídia contendo os dados pessoais devem ajudar a identificar o tipo de informação que contêm e ser inventariados, serão armazenados no servidor Linux, em vez de restringir o acesso apenas ter acesso ao pessoal que está autorizado a este fim, sempre dependendo do super-administrador.

Backups: Backups são realizados em uma base diária, e podem ser restauradas imediatamente (com uma margem de duas horas) de dados com um aviso prévio de 7 dias. Arquivos contêm armazenados como software de banco de dados subjacente à camada de usuário plataforma RESATER. Os procedimentos para backups assegurar a sua reconstrução no estado em que foram produzidos na época da perda ou destruição, bem como qualquer versão do backup que você quer de 7 dias anteriores.

Security Officer: Um oficial de segurança designado dentro da RESATER consórcio, ou se for o caso, o super administrador do sistema, que geralmente é responsável pela coordenação e monitoramento das medidas definidas no documento de segurança.

CAPÍTULO 3: PROCEDIMENTO GERAL DE INFORMAÇÕES AOS USUÁRIOS.

Para garantir que todos os usuários estão cientes das normas de segurança que afetam o

desempenho de suas funções, este documento pode ser visível ou distribuídos através da plataforma e do RESATER Observatório criado para esta finalidade.

CAPÍTULO 4: FUNÇÕES E DEVERES DOS USUÁRIOS.

Todos os usuários que acessam o consórcio RESATER plataforma são necessários para conhecer e observar as medidas, normas e procedimentos que afetam as funções que ele executa.

Todos os usuários devem observar o sigilo adequado e confidencialidade dos dados pessoais estão cientes do desenvolvimento de seu trabalho.

CAPÍTULO 5: PROCEDIMENTO DE NOTIFICAÇÃO, gerenciar e responder a incidentes.

São consideradas "incidentes de segurança", entre outros, qualquer violação das regras previstas no presente documento de segurança, e qualquer alteração que afetam ou podem afetar a segurança dos dados pessoais associadas profissionais consórcio RESATER.

CAPÍTULO 6: RECURSOS.

O documento de segurança serão analisadas pelo oficial de segurança designado em intervalos não superiores a 30 dias, estabelecendo assim um controle de folha de "manual" para servir como a avaliação dos registros e incidentes causados, sendo atualizada em todos os momentos. Na verdade, deve ser revisto sempre que ocorram alterações significativas no sistema de informação, o conteúdo das informações contidas em ficheiros ou como resultado das inspeções periódicas executadas.

Tabela 1. Segurança dos documentos - Regulamento.

As folhas a serem preenchidos devem apresentar o seguinte formulário. Ele detalha o tipo de incidente (se isso fosse uma revisão regular, encher a caixa correspondente a "relatórios periódicos"), o número de revisão, o tipo de usuário que teve o impacto (para

identificar o papel de acesso à plataforma) e seu nome ea data da ocorrência ea causa razão da revisão, a mais extensa do que no título original.

Tipo de Incidente:				
Revisão	Tipo de usuário	Nome	Data	Razão

Tabela 2. Relatório de Segurança (para completar)

Com esse monitoramento sobre a incidência e os profissionais o acesso à plataforma do consórcio terá um desempenho constante RESATER e avaliação de usabilidade que fornece toda a plataforma.

Da mesma forma, o oficial de segurança irá preparar uma lista de usuários (com diferentes tipos de licenças) para ser atualizado com todas as alterações ou notícias que têm impacto sobre a lista de pessoas que têm acesso à plataforma.

Privacidade Sala Virtual.

A plataforma RESATER virtuais quarto é um dos módulos que compõem a plataforma de profissionais. Ele pode fornecer videoconferência e bate-papo, a fim de permitir que todos os usuários a participar neste espaço de colaboração internacional, alcançando assim a interoperabilidade entre os profissionais para uma melhor prestação de serviços relacionados.

A privacidade que você esta sala está em linha com outras medidas de segurança no ambiente de plataforma profissionais. A operação da carta é a seguinte:

1. Profissionais associados com a plataforma pode constituir um vídeo e enviar convites a outros profissionais que têm o seu próprio login e senha para acessar a plataforma, tais como profissionais externos aos quais o url de validação de acesso chegará por e-mail.

2. Uma vez que os convites enviados a uma sessão de videoconferência particular, na casa de profissionais vai ver o convite em seu "video vista" e acessá-lo uma vez ativado.
3. A segurança deste sistema restringe o criador do vídeo como o primeiro profissional para acessá-lo. Os usuários convidados outros têm acesso depois de ter feito essa validação. Internamente, o sistema tem três níveis de acesso para verificar as permissões para cada usuário sobre o assunto.
4. Quando um acesso usuário convidado é verificado (a um nível inferior) com um "token" que o hóspede está no banco de dados da videoconferência. No caso de você não ter começado, você receberá uma mensagem indicando este estado.
5. Se houver um "intruso" ganha acesso à url onde o vídeo será estabelecido, mas não foi convidado pelo criador, a tela mostrará a não inclusão na base de dados do mesmo, negando o acesso apropriado. Este tipo de segurança para proteção abrangente que você não pode fazer uso malicioso do acesso a uma sessão dentro da sala virtual.

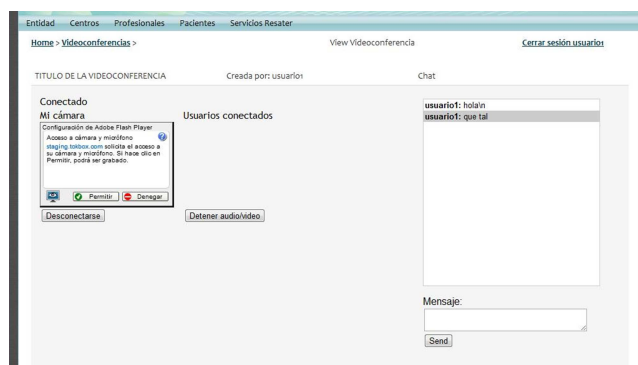
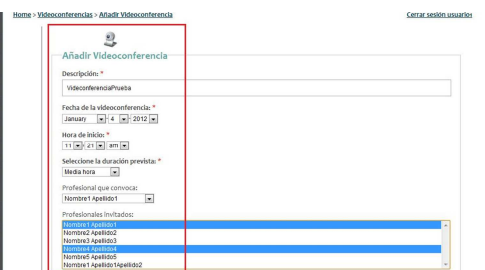
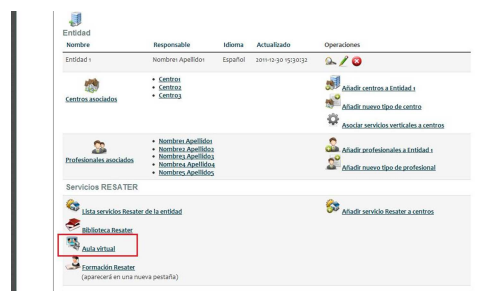


Figura 3. Acesso a um módulo Virtual Sala de Videoconferência

Conclusões

A segurança associados ao consórcio plataforma de telemedicina RESATER é um dos principais para a implementação adequada do mesmo. Conformidade com a legislação europeia sobre os sistemas de comunicação on-line e tratamento de dados pessoais que regulamenta a matéria com grande disciplina dentro do quadro legal, referindo-se aos países da Espanha, França e Portugal. É por isso que todo o acesso a bases de dados e informações "sensíveis" é regido pela limitação e controle de usuários registrados e requisitos de licenciamento associados com cada um.

O sistema irá validar o acesso à plataforma, primeiro, que estabelece, através de uma "validação da cadeia tem" recebido no e-mail em si, o que confirmou a incorporação de um novo usuário para o sistema de banco de dados. Este processo de segurança foi desenvolvido através de um ambiente próprio desenvolvimento CakePHP hash, alcançando assim uma alta confiabilidade na segurança implícita que a plataforma de software tem. O sistema de licenças utilizados para este fim é chamado ACL, e colocar em relação ao ACOs e AROs criado, que estrutura os usuários em grupos diferentes, cada um com um conjunto de privilégios específicos.

Em termos de medidas técnicas e arranjos organizacionais em relação à segurança de arquivos compartilhados e bancos de dados criados, considerados três tipos de níveis: baixa, média e alta. A primeira considera os dados pessoais, gravado sobre as formas iniciais de coleta de dados. O nível médio concentra-se em informações do usuário por meio de identificação pessoal armazenadas, com acesso limitado a praticamente todos os usuários. Finalmente, de alto nível medidas não foram contemplados neste espaço colaborativo para ter uma natureza diferente da prevista na descrição do uso e da finalidade da plataforma RESATER consórcio.

O documento de segurança (e as regras envolvidas) procura identificar um conjunto de procedimentos a todos os usuários e / gerentes / s dos documentos armazenados dentro das diretrizes estabelecidas. Essas são medidas básicas que ajudam a fortalecer as garantias de segurança do software desenvolvido, a fim de atualizar e melhorar o funcionamento da plataforma e, portanto, é um pedido dinâmica e altamente escalável para qualquer mudança.

Finalmente, a privacidade associados à Plataforma Sala Virtual fortalece ainda mais a impossibilidade de fazer uso malicioso de seus recursos, permitindo o acesso a vídeo, a pessoas que não estão associados com a RESATER consórcio (mas considera que um

profissional de internos deveria ser) em uma visão paralela, garantindo o acesso a todo o momento através do banco de dados criado para identificar os usuários convidados para a sessão.

Referências

- [1] <http://cakephp.org>
- [2] <http://www.aepd.es>
- [3] <http://www.tokbox/opentok/>
- [4] Estudo 3. "Lei plataforma RESATER Firm"