SREI

Sistema de Registro Eletrônico Imobiliário

Parte 3 – Certificação de software SREI

C – Roteiro de ensaios para avaliação da conformidade do software SREI

Título	SREI Parte 3 C – Roteiro de ensaios para avaliação da conformidade do software SREI
Versão	Versão 1.2 release 2
Data da liberação	30/05/2012
Classificação	Restrito
Autores	Gislaine Bueno, Volnys Bernal
Propriedade	CNJ
Restrições de acesso	LSI-TEC, CNJ e ARISP

Sumário

1 Introdução

Este documento descreve o roteiro de ensaios utilizados para verificar a aderência do SREI aos requisitos de segurança, os quais foram descritos no documento “Requisitos técnicos para software SREI”.

2 Roteiro de ensaios para avaliação de conformidade

Esta seção descreve o roteiro de ensaios para avaliação de conformidade do software SREI em relação aos requisitos definidos.

2.1 Segurança

As seções a seguir apresentam os ensaios que devem ser utilizados para avaliar os requisitos relacionados à segurança do SREI.

No contexto deste documento, o termo “registro” possui duplo sentido. Pode se referir ao “registro imobiliário” ou ao “registro de eventos” no sentido de log. Para evitar esta situação, sempre que possível, quando for necessário se referir ao “registro de logs” será utilizado o termo “anotação de evento”.

Os ensaios estão distribuídos conforme a estrutura utilizada para descrever os requisitos:

- Controle de versão do software;
- Gerenciamento de usuários;
- Identificação e autenticação dos usuários;
- Controle da sessão do usuário;
- Autorização e controle de acesso;
- Integridade e disponibilidade dos registros eletrônicos;
- Segurança dos canais de comunicação;
- Rastreabilidade dos eventos;
- Tempo;
- Notificação de ocorrências;
- Documentação do software.

2.1.1 Controle de versão do software

A utilização de controle da versão do software possibilita associar problemas, funcionalidades e estágio de certificação a uma determinada versão. É um controle importante para a segurança do ciclo de vida do software e, também, para o processo de certificação do software.

ID	Ref	Requisito	Descrição
SEG.E001	SEG.CV.01	Versão do software	**PR:** Verificar se o SREI possui recurso para visualizar a nome, fornecedor e número da versão do software em uso. **RE:** Estas informações devem estar contidas no SREI e devem ser acessíveis ao usuário
SEG.E002	SEG.CV.02	Controle de versões do software	**PR:** Verificar se o SREI possui recurso de repositório estruturado **RE**: O fornecedor DEVE possuir um repositório estruturado contendo todas as versões dos componentes (executáveis e códigos-fonte).

2.1.2 Gerenciamento de usuários

ID	Ref	Requisito	Descrição
SEG.E003	SEG.GU.01	Identificação única do usuário	**PR:** Verificar se o sistema é capaz de identificar de forma unívoca os usuários cadastrados no sistema; 1) Verificar se o sistema é capaz de localizar e diferenciar homônimos; 2) Verificar se o sistema possui controle de duplicidade. a. Inserir um novo usuário preenchendo todos os campos (estado, nome, CPF,

			etc) Deve ser realizada a validação do número do CPF inserido; b. Em um segundo momento, tentar inserir um novo usuário com o mesmo identificador, CPF, etc. c. Desativar o usuário criado no item “a” e repetir a operação sugerida no item “b” **RE:** Item 1 – Operação deve ser possível Item 2 – a. Deve ser realizado com sucesso; b e c. O sistema não deve permitir o sucesso das operações contidas nesses itens.
SEG.E004	SEG.GU.02	Gerenciamento de usuários	**PR**: 1) Acessar o sistema com o usuário administrador e criar dois usuários; 2) Atribuir papéis distintos aos usuários recém-criados, como exemplos; - “Atendente”; - “Escrevente”; 3) Criar dois grupos distintos e inserir cada usuário em um grupo 4) Solicitar o acesso ao sistema com os usuários criados para atestar a criação e atribuições dos papéis e grupos R: Deve ser possível criar usuários, atribuir papéis e grupos
SEG.E005	SEG.GU.02	Gerenciamento de usuários	**PR:**

			Acessar o sistema com o usuário administrativo e realizar as seguintes operações: 1) Modificar o usuário com papel de “Atendente” para o papel de “Operador”; 2) Desabilitar o usuário com papel de “Atendente” **RE:** Todas as operações DEVEM ser realizadas com sucesso, comprovando a possibilidade de gerenciamento de usuários, papéis e grupos.
SEG.E006	SEG.GU.02	Gerenciamento de usuários	**PR:** Autenticar no SREI utilizando o usuário com papel de “Atendente” e tentar acessar as informações restritas somente ao “Oficial” **RE:** O sistema não DEVE permitir o acesso.
SEG.E007	SEG.GU.03	Remoção de usuários	**PR**: 1) Acessar o SREI com o usuário Administrador de TI e tentar excluir o usuário “Atendente”; 2) Ainda com o usuário “Administrador”, inativar o usuário “Atendente” e tentar excluí-lo. **RE**: O SREI NÂO DEVE permitir a exclusão do usuário. O SREI DEVE permitir desabilitar o usuário
SEG.E008	SEG.GU.04	Papeis de usuários	**PR**: 1) Criação de Grupos Criar grupos de usuários considerando as funções exercidas: • Solicitante • Operador de registro imobiliário • Operador de TI • Corregedor

			2) Criação de usuários:
			Criar os seguintes usuários e inseri-los nos grupos correspondentes:
			• Solicitante:
			  ○ Cliente
			• Operador de registro imobiliário:
			  ○ Oficial;
			  ○ Escrevente;
			  ○ Atendente;
			  ○ Gestor
			• Operador de TI:
			  ○ Administrador TI;
			  ○ OperadorTI;
			  ○ OperadorBackup;
			  ○ AuditorTI;
			• Corregedoria
			  • Corregedor
			RE: O SREI deve permitir a criação de grupos e usuários, considerando os devidos privilégios de acesso.

SEG.E009	SEG.GU.04	Associação de usuário a múltiplos perfis	**PR**: Acessar o sistema com o usuário “Administrador “ e a um mesmo usuário atribuir os perfis: • Oficial; • Escrevente; **RE**: DEVE ser possível atribuir mais de um perfil de acesso ao mesmo usuário.

2.1.3 Identificação e autenticação dos usuários

A identificação dos usuários permite discriminar cada usuário individualmente em um acesso ao sistema. Nos sistemas de software, a identificação é realizada através da associação de um identificador de usuário à pessoa.

A autenticação de usuário é o ato de confirmar uma identidade alegada por uma pessoa. A autenticação pode utilizar um ou mais fatores de autenticação, baseado em conhecimento, posse ou característica da pessoa.

	Ref	Requisito	Descrição
SEG.E010	SEG.IAU.01	Identificação e autenticação do usuário	**Teste 1) Interface para acesso de usuários restritos/cadastrados no sistema** **PR:** Verificar que o acesso ao sistema SRES é possível unicamente por meio de interface de identificação e autenticação de usuário. . **RE:** O SREI deve ser acessível somente através da interface de identificação de usuário. No caso de autenticação por Usuário/senha o S-RES deve permitir o acesso somente apos a inserção do usuário e da senha.
SEG.E011	SEG.IAU.01	Identificação e autenticação do usuário	**Teste 2) Identificação e autenticação via usuário e senha** **PR:** No caso que o sistema de autenticação seja por meio de senha, verificar que o sistema possua uma interface para inserção de usuário e senha **RE**: O SREI DEVE permitir o acesso somente após a inserção do usuário e da senha.
SEG.E012	SEG.IAU.01	Identificação e autenticação do	**Teste 3) Identificação e autenticação via Certificado Digital** **PR:** Entrar no sistema com perfil de operador.

		usuário	**RE:** Deve ser necessário o uso do certificado digital ICP-Brasil para realizar essa ação
SEG.E013	SEG.IAU.01	Identificação e autenticação do usuário	**Teste 4) Acesso às operações ou informações de caráter público** **PR:** Acessar o sistema e tentar obter acesso a operações ou informações de caráter público irrestrito. **RE**: O SREI DEVE prover o acesso livre a este tipo de operações ou informações.
SEG.E014	SEG.IAU.02	Método de autenticação do usuário	**PR:** Verificar se o sistema utiliza, no mínimo, um dos seguintes métodos de autenticação: 1 - Usuário/senha 2 - Certificado Digital **RE**: O SREI deve utilizar ao menos um dos métodos de autenticação citados acima.
SEG.E015	SEG.IAU.03	Procedimento de entrada no sistema (*login*)	**Teste 1) Aviso de acesso ao sistema** **PR**: Verificar se o SREI exibe o aviso que somente usuários autorizados DEVEM acessar o sistema. **RE**: O SREI deve exibir o aviso de acesso ao sistema.
SEG.E016	SEG.IAU.03	Procedimento de entrada no sistema (*login*)	**Teste 2) Bloqueio de usuários após tentativas de entrada no sistema incorreta:** **PR**: Verificar se o SREI possui recurso de bloqueio de acesso de usuário após número de tentativas mal sucedidas configurável. • Configurar o número máximo de tentativas falhas de login para 3 ; • Efetuar 3 tentativas de acesso com senhas incorretas utilizando o usuário com papel de “Atendente”; • Acessar o SREI com o usuário que possui o papel de “Atendente”, utilizando a senha correta; • Constatar se o acesso do usuário com papel de “Atendente” foi bloqueado;

			RE: O número de tentativas falhas deve ser configurável e o sistema deve bloquear o acesso ao usuário após o número de tentativas definido.
SEG.E017	SEG.IAU.03	Procedimento de entrada no sistema (*login*)	**Teste 3) Tempo máximo permitido para a entrada:** **PR**: Verificar se o SREI possui recurso configurar o tempo máximo permitido para entrada **RE**: O limite de tempo máximo permitido para o procedimento de entrada deve ser parametrizável.
SEG.E018	SEG.IAU.03	Procedimento de entrada no sistema (*login*)	**Teste 4) Informações de acesso:** **PR**:Verificar se o SREI exibe informações de acesso: o Instante da última entrada no sistema (*login*) com sucesso; o Detalhes de tentativas de entrada no sistema (*login*) sem sucesso, desde a última entrada com sucesso. **RE:** O SREI DEVE exibir as informações de acesso.

SEG.E019	SEG.IAU.04	Proteção dos parâmetros de autenticação	**Teste 1) Proteção da senha** **PR:** Levantar qual a forma de armazenamento e a localização no SREI dos parâmetros de autenticação, 1 - Usuário/senha a - Verificar que seja armazenado unicamente o código hash da senha. b - Verificar que o tipo de algoritmo de codificação hash utilizado é um algoritmo padrão seguro. c - Verificar a partir do usuário BDRestrito se somente o usuário administrativo possui acesso aos códigos hash das senhas dos usuários do SREI Estas recomendações devem estar contidas na documentação do software.
SEG.E020	SEG.IAU.04	Proteção dos parâmetros de autenticação	**Teste 2) Proteção do Certificado Digital:** **PE**: Verificar que o sistema que armazena o certificado necessite de uma autenticação antes. **RE**: O repositório de certificados deve ser acessível somente através de autenticação.
SEG.E021	SEG.IAU.04	Proteção dos parâmetros de autenticação	**Teste 3) Documentação relacionados aos parâmetros de autenticação** **PR:** Verificar se a documentação contempla a configuração dos parâmetros de autenticação.
SEG.E022	SEG.IAU.04	Proteção dos parâmetros de autenticação	**Teste 4) Armazenamento dos dados ou parâmetros críticos** **PR**: Verificar o local de armazenamento dos dados ou parâmetros críticos utilizados no processo de autenticação. **RE**: Os dados ou parâmetros críticos devem ser armazenados separadamente dos dados do sistema da aplicação.
SEG.E023	SEG.IAU.05	Autenticação	**PR**:

		por senha: procedimento de entrada no sistema (*login*)	Acessar o SREI e verificar: a. Se é possível visualizar a senha informada pelo usuário; b. Utilizar uma ferramenta de snnifing para capturar a senha informada pelo usuário e verificar se a senha é passada em texto claro; c. Nos acessos realizados no item d, verificar as mensagens de erro retornadas pelo sistema e ainda validar as mensagens realizando os seguintes acessos: • Inserir usuário correto e senha incorreta; • Inserir usuário incorreto e senha correta. d. Verificar se é possível acessar o sistema nas seguintes situações: • Inserindo somente a senha, deixando o campo usuário em branco; • Inserindo somente o usuário, deixando campo senha em branco; • Inserindo usuário e senha em branco; Validar todos os campos necessários para identificação e autenticação no sistema; **RE**: O SREI não DEVE permitir o sucesso dos itens “a” e “b” As mensagens de erros geradas no item “c” e “d” não deve evidenciar em qual campo ocorreu o erro.
SEG.E024	SEG.IAU.06	Autenticação por senha: proteção dos parâmetros críticos	**PR**: Verificar os mecanismos utilizados para proteção de parâmetros críticos. 1 - Deve ser forçada a utilização de senha com, no mínimo, 8 caracteres e dentre estes ao menos 1 não-alfanumérico. 2 - . Se é possível o usuário modificar sua própria senha e se é possível confirmar a nova senha; 3 – Utilização de mecanismos de proteção para base de armazenamento da codificação das

	SEG.IAU.08	Autenticação por senha: qualidade da senha	senhas; 4 – O SREI deve forçar o usuário a trocar sua senha em um período máximo configurável, e a nova senha não pode ser igual a(s) anterior(es), conforme parametrizado no sistema. **RE**: Todos os itens devem ser atendidos
	SEG.IAU.10	Autenticação por senha: periodicidade da troca de senhas	
	SEG.IAU.11	Autenticação por senha: reutilização da senha:	
SEG.E025	SEG.IAU.09	Autenticação por senha: análise de dicionário	**PR**: Verificar se o SREI verificar a qualidade da senha, visando evitar ataques de dicionários. **RE**: Todos os itens devem ser atendidos
SEG.E026	SEG.IAU.12	Autenticação por certificado digital: segredo da chave privada	**Teste 1)** **PR:** Com usuários com privilégio de realizar operações de autenticação, utilizar um certificado digital ICP-Brasil COM propósito de autenticação e realizar uma operação de autenticação. **RE**: O Sistema DEVE permitir a realização da atividade verificando se a chave privada é de conhecimento e acesso único do usuário.
SEG.E027	SEG.IAU.12	Autenticação por certificado digital: segredo da chave privada	**Teste 2)** **PR:** Com usuários com privilégio de realizar operações de autenticação, utilizar um certificado digital ICP-Brasil SEM propósito de autenticação e realizar uma operação de autenticação. **RE:** O Sistema não deve permitir a realização da atividade, emitindo uma mensagem de erro

			apropriada.
SEG.E028	SEG.IAU.13	Autenticação por certificado digital: validação do certificado digital	**PR**: Realizar os seguintes testes: 1 - Operação de autenticação com certificado digital vencido; 2 - Operação de autenticação com certificado digital revogado; 3 - Operação de autenticação com certificado digital com problema de integridade; RE: Sistema deve impedir todas essas operações e informar o usuário sobre o problema
SEG.E029	SEG.IAU.14	Autenticação por certificado digital: Irretratabilidade da autenticação:	**PR:** Realizar uma operação de autenticação, verificar a existência do registro de irretratabilidade gerado. Exportar tal registro e validá-lo em um programa de validação de assinatura digital. **RE**: O registro deve ser validado com sucesso, contendo todos os elementos para a validação.
SEG.E030	SEG.IAU.15	Autenticação por certificado digital: requisitos ICP-Brasil	**PR**: Com um certificado de sigilo, realizar uma operação de autenticação de usuário. Selecionar um usuário com privilégios para realizar tais operações. **RE**: O sistema deve impedir a operação, informando ao usuário que o certificado não possui propósito suficiente para realizar a operação de autenticação ou de assinatura digital.
SEG.E031	SEG.IAU.16	Autenticação por certificado digital: homologação ICP-Brasil	**PR**: 1) Utilizar um certificado digital ICP-Brasil, para realizar duas atividades, com usuários que tenham privilégio de: a. Uma autenticação 2) Utilizar um certificado digital não ICP-Brasil, para realizar duas atividades: a. Uma autenticação **RE**: Sistema deve permitir a realização da operação 1a e não permitir as operações 2a.

SEG.E032	SEG.IAU.17	Autenticação por certificado digital: certificado ICP-Brasil:	**PR**: Verificar se o sistema possui ou utiliza um repositório específico para gerenciamento dos certificados raiz de confiança. Verificar se este repositório possui controles de acesso e/ou integridade para gerenciar os certificados raiz de confiança. **RE**: Sistema deve permitir o controle e gerenciamento dos certificados raiz de confiança. Observação: A cadeia de certificado, em algumas situações, poderá ser de outra cadeia, por exemplo, na situação de convênios com entidades do exterior.
SEG.E033	SEG.IAU.18	Autenticação dos funcionários	**PR**: Verificar se todos os acessos realizados pelos usuários do cartórios utilizam certificados digitais **RE**: Para os usuários associados aos funcionários o SREI DEVE exigir o uso de certificado digital

2.1.4 Controle da sessão do usuário

A sessão do usuário corresponde à sequência de interações que ocorrem entre o usuário e sistema, da sua autenticação até o encerramento da sua interação com o sistema.

	Ref	Requisito	Descrição
SEG.E033	SEG.CSU.01	Controle da sessão do usuário	**PR**: Durante o acesso ao SREI, utilizar ferramenta de interceptação analisar em quais momentos são utilizados os mecanismos de controle de sessão, considerando o período de autenticação até o encerramento da sessão do usuário. **RE**: O sistema DEVE realizar o controle da sessão do usuário, desde a autenticação do usuário até o encerramento da sua sessão de uso.

SEG.E034	SEG.CSU.02	Segurança contra roubo da sessão do usuário	**Teste 1)Condicional a Aplicação WEB** **PR**: 1) Acessar o SREI com o usuário que possui papel de Oficial, utilizando uma ferramenta de interceptação, capturar o token (s) utilizado(s) durante a sessão do usuário. 2) Acessar SREI com o usuário com o usuário que possui o papel de AdministradorTI, utilizando a ferramenta de interceptação e trocar token (s) por aquele (s) capturado na sessão usuário que possui papel de Oficial. **RE**: O sistema não deve permitir a troca dos tokens de sessão
SEG.E035	SEG.CSU.02	Segurança contra roubo da sessão do usuário	**Teste 2) Condicional a Aplicação WEB** **PR**:Verificar que em nenhum momento de uso do sistema o Token de sessão, tal como outras informações de credencial de acesso, são enviados como parâmetro na URL (o teste se aplica somente no caso de aplicações web). **RE:** O token de sessão deve ser enviado no cabeçalho da mensagem como parâmetro da variável cookie ou outra variável ou ainda no corpo da mensagem.
SEG.E036	SEG.CSU.03	Encerramento por inatividade	**PR**: Verificar se o tempo de timeout da sessão é parametrizável. Caso seja, definir como 3 minutos, acessar o sistema e deixar o usuário inativo por este período. Após este período, verificar se a sessão permanece válida, permitindo ao usuário navegar e utilizar os recursos normalmente. Caso o tempo de timeout não seja parametrizável, levantar qual o tempo de timeout da sessão do usuário e, sucessivamente, verificar se houve o encerramento da sessão após o timeout. **RE**: A sessão deve possuir timeout de sessão de usuário definido e deve ser encerrada após este período.
SEG.E037	SEG.CSU.04	Invalidação após encerramento	**PR:** 1) Realizar acesso ao SREI e utilizando uma ferramenta de interceptação, capturar o

		do objeto de controle de sessão	cookie utilizando para controle da sessão e sair da aplicação (logout[1]); 2) Realizar acesso ao SREI e utilizando uma ferramenta de interceptação, capturar o cookie e forçar o timeout[2] da aplicação; 3) Realizar acesso ao SREI e utilizando uma ferramenta de interceptação, forçar o uso do cookie capturado antes de efetuar o logout da aplicação; 4) Realizar acesso ao SREI e utilizando uma ferramenta de interceptação, forçar o uso do cookie capturado antes de efetuar o timeout da aplicação; **RE:** O sistema não deve permitir o reuso do controle da sessão do usuários após o encerramento da sessão.
SEG.E038	SEG.CSU.05	Previsibilidade do objeto de controle de sessão	**Teste 1)Condicional a Aplicação WEB** **PR**: Executar 10 logins sucessivos com o usuário administrativo, coletar os relativos Tokens de sessão e verificar se não há uma seqüência lógica entre os Tokens (o teste se aplica somente no caso de aplicações web). **RE**: O Token de sessão deve ser diferente a cada nova sessão e não deve ser possível encontrar uma lógica que possibilite prever os Tokens sucessivos.
SEG.E039	SEG.CSU.06	Limitação de horário para determinadas operações	PR:Acessar o sistema com o usuário com o papel de AdministradorTI e restringir o acesso do usuário com papel de “Atendente” apenas para o período das 09:00 as 10:00. Tentar acessar o sistema, utilizando o usuário com papel de “Atendente”, fora do período estipulado.

[1] Finalização da sessão executada pelo usuário ao selecionar a opção sair ou fechar o sistema.

[2] Expiração de sessão após tempo de inatividade configurável.

			RE: O sistema não DEVE permitir o acesso fora do período estipulado.

2.1.5 Autorização e controle de acesso

A autorização representa a habilidade de definir quais entidades (pessoa ou processo) podem fazer uso de um recurso (operação, dado, etc).

O controle de acesso representa a habilidade de permitir ou negar a utilização de um recurso (operação, dado, etc) por uma entidade (pessoa ou processo) autenticada.

ID	Ref	Requisito	Descrição
SEG.E040	SEG.ACA.01	Impedir o acesso por entidades não autorizadas	**PR:** Acessar com o usuário que possui o papel de AuditorTI (perfil Auditor) e verificar: a - Se possui acesso aos registros de auditoria do SREI b - Que não pode realizar atividades administrativas no SREI como cadastrar usuário, alterar perfil, alterar nívelacesso etc. c - Que não existe algum recurso no SREI que permite a inserção de dados nos registros eletrônicos imobiliários. **RE:** Não deve ser possível obter acesso a funcionalidades não-autorizadas a este usuário.
SEG.E041	SEG.ACA.02	Configuração do controle de acesso	**PR:** Sair do sistema e acessar como usuário AdministradorTI para verificar se há possibilidade de conceder autorização e definir controle de acesso para o usuário com papel de “Atendente”. 1 - Alterar o perfil do usuário de “Escrevente” para "Oficial" 2 - Sucessivamente entrar no SREI com o usuário com papel de Oficial e verificar se possui capacidade de realizar as atividades inerentes ao Oficial.

ID	Ref	Requisito	Descrição
			RE: Deve ser possível para o AdministradorTI conceder autorizações e definir controle de acesso ao usuário deacordo com a necessidade.
SEG.E042	SEG.ACA.03	Controle de acesso aos dados do SREI	**Teste 2) Acesso à base de dados** **PR**: 1 - Por meio de um cliente de BD compatível com a solução utilizada, realizar conexão com o BD e verificar se é possível acessar as bases de dados: a - Sem autenticação b - A partir de usuários padrão do BD 2 - Verificar que não existem outras aplicações ou módulos do SREI, fora do escopo do processo de auditoria, que podem acessar a base de dados que hospeda o REI. Verificar se estas recomendações estão contidas na documentação do software. **RE:** O sistema NÃO DEVE permitir acesso aos dados do SREI por canais não autorizados Não DEVE ser possível acessar bases de dados sem autenticação, e os usuários padrão do BD devem ser desabilitados ou ter suas credenciais de acesso alteradas (quando aplicável). Devem constar estas recomendações de segurança na documentação do software.

ID	Ref	Requisito	Descrição
SEG.E043	SEG.ACA. 04	Delegação de privilégio	**CD:** Este *script* é diretamente relacionado à política de negócio e, caso esta não objetive a delegação de poder, este *script* não DEVE ser executado. **Teste 1)** **PR:** 1 – Acessar o SREI com o usuário com o papel de “Oficial”, atribuir ao usuário com papel de "Escrevente" o poder assinar digitalmente os registros eletrônicos imobiliário. 2 – Determinar o prazo de vigência do poder delegado; 3 - Formalizar a delegação de privilégio. 4 - Acessar o SREI a partir do usuário com papel de "Escrevente" e verificar se é possível assinar digitalmente os registros eletrônicos gerados **RE:** O sistema DEVE verificar se o atribuidor está previamente autorizado a delegar o privilégio. Deve ser possível para o usuário “Escrevente” assinar digitalmente os registros gerados.
SEG.E044	SEG.ACA. 04	Delegação de privilégio	**CD:** Este *script* é diretamente relacionado à política de negócio e, caso esta não objetive a delegação de poder, este *script* não DEVE ser executado. **Teste 2)** **PR**: Acessar o documento assinado digitalmente, que representa a formalização da delegação de poder e verificar se o documento está armazenado em local apropriado. **RE**: O sistema DEVE suportar a formalização da atividade de delegação de privilégio e armazenar adequadamente o documento assinado digitalmente gerado.
SEG.E045	SEG.ACA. 04	Delegação de privilégio	**CD:** Este *script* é diretamente relacionado à política de negócio e, caso esta não objetive a delegação de poder, este *script* não DEVE ser executado. **Teste 3)** PR: 1- Alterar o prazo de vigência atribuído no Teste 1 para um dia anterior a data atual; 2 – Acessar o sistema com o usuário com papel de “Escrevente” RE: O sistema não DEVE permitir o usuário assine digitalmente os registros gerados.

ID	Ref	Requisito	Descrição
SEG.E046	SEG.ACA. 04	Delegação de privilégio	**CD:** Este *script* é diretamente relacionado à política de negócio e, caso esta não objetive a delegação de poder, este *script* não DEVE ser executado. **Teste 4)** **PR:** A partir de um usuário com papel "AuditorTI", verificar a existência dos eventos a partir da atividade de delegação de poder, considerando: • O atribuidor; • O delegado; • O motivo; • O instante da delegação; • O período de vigência. **RE:** As trilhas de auditoria devem conter, no mínimo, as informações relacionadas acima.

2.1.6 Integridade e disponibilidade dos registros eletrônicos

ID	Ref	Requisito	Descrição
SEG.E047	SEG.IDR.01	Verificação da integridade dos livros eletrônicos	**PR**: 1 - Reinicializar o sistema e verificar se o sistema realiza a atividade de verificação de integridade dos livros eletrônicos; 2 – Averiguar em quais momentos é verificada a integridade dos livros eletrônicos. **RE**: O sistema DEVE verificar a integridade na iniciação do sistema e também, ao menos uma vez ao dia.
SEG.E047	SEG.IDR.02	Verificação da integridade dos registros	**PR:** Verificar se o SREI possui controle que permita verificar a integridade dos dados da base de livros eletrônicos e verificar se a periodicidade assumida pelo sistema está de acordo com a configurada.

ID	Ref	Requisito	Descrição
		eletrônicos	**RE:** O SREI DEVE garantir a verificação de integridade dos dados conforme periodicidade definida no sistema.
SEG.E048	SEG.IDR.03	Exportação dos registros eletrônicos	**Teste 1)** **PR**: Exportar os registros eletrônicos e verificar: 1- Estrutura hierárquica; 2- Metadados ou nó de agrupamentos exportados; 3- Verificar o formato de arquivo exportado. **PE**: Todos os elementos DEVEM estar presentes nos registros eletrônicos exportados.
SEG.E049	SEG.IDR.03	Exportação dos registros eletrônicos	**Teste 2)** **PR:** 1) Verificar o registro, utilizando um aplicativo de verificação de assinatura se ele possui todos os elementos necessários para a validação da assinatura. **RE:** Todos os elementos necessários para a validação da assinatura devem estar presentes
SEG.E050	SEG.IDR.04	Importação dos registros eletrônicos	**PR:** Executar as seguintes atividades: 1- Importar a "base-teste" no SREI 2- Verificar que os dados importados pertençam estavam de acordo; 4- Verificar que exista nos registros (logs) do SREI seja registrada a atividade de importação contendo no mínimo as seguintes informações: a. Data e hora da importação b. Equipamento de onde foi realizada a importação c. Usuário do SREI **RE:** Todos os itens deste *script* devem ser atendidos.
SEG.E051	SEG.IDR.05	Impedir exclusão e modificação de	**PR:** Logar no SREI como administrador e verificar que: a. Não existam recursos para remoção total ou parcial de dados do REI b. Não hajam recursos para a alteração de dados do REI

ID	Ref	Requisito	Descrição
		registros eletrônicos	Acessar o sistema com usuário que possui papel de “Oficial” e verificar que: a. Acessar um registro de eletrônico de um determinado imóvel. b. Tentar inserir alterar ou excluir um registro eletrônico já assinado. **RE:** Não deve ser possível remover, alterar ou sobrescrever informações contidas no SREI Ações de correção DEVEM sempre preservar os dados anteriores.

2.1.7 Segurança dos canais de comunicação

ID	Ref	Requisito	Descrição
SEG.E052	SEG.SCC.01	Segurança da comunicação de componentes remotos para acesso do usuário	**PR:** Caso o sistema disponibilize um componente remoto para viabilizar a interação com o usuário, verificar se é utilizado o protocolo HTTPS durante conexão. No caso da utilização do HTTPS, testar ao longo da navegação se em um dado momento é possível forçar o acesso ao endereço através do protocolo HTTP. **RE:** Deve ser recomendada e estar implementada a utilização de protocolo seguro durante a conexão com o servidor
SEG.E053	SEG.SCC.02	Segurança da comunicação entre componentes distribuídos	**PR:** Verificar se há alguma restrição de acesso entre os componentes. a - Verificar através de um cliente de BD compatível com o BD em análise se somente requisições realizadas a partir do servidor de aplicação são aceitas pelo servidor de BD. b - No caso de webservices verificar se ha autenticação entre os componentes. **RE:** O acesso entre os componentes deve ser restrito somente aos componentes previamente autorizados.
SEG.E054	SEG.SCC.03	Segurança da comunicação	**PR**:Verificar as restrições de acesso para comunicação entre o SREI e as entidades externas.

ID	Ref	Requisito	Descrição
		com entidades externas	**RE**: Os serviços de segurança DEVEM ser garantidos: a autenticação de parceiro, integridade e confidencialidade dos dados.

2.1.8 Rastreabilidade dos eventos

A rastreabilidade dos eventos que ocorreram no sistema é possível quando são gerados e mantidos anotações[3] adequadas sobre os eventos (logs) que ocorreram no sistema.

ID	Ref	Requisito	Descrição
SEG.E055	SEG.RE.01	Geração contínua de anotações de eventos (*logs*)	**PR:** Verificar se o SREI possui recursos que possibilitem a desativação, alteração, remoção ou substituição totais ou parciais das trilhas de auditoria. No caso de SGBD, verificar se somente o usuário de auditoria tem acesso às trilhas de auditoria, e se este acesso somente permite consulta. **RE:** Não pode haver recursos que possibilitem a desativação, alteração, remoção ou substituição total ou parcial das trilhas de auditoria. Somente o auditor deve ter acesso às

[3] Neste documento o termo “anotação” será utilizado preferencialmente em substituição ao termo “registro” (“log”) quando se referir a registro de eventos, a fim de diferenciar do “registro eletrônico imobiliário”.

ID	Ref	Requisito	Descrição
			trilhas de auditoria, e este acesso somente deve permitir consulta das informações.
SEG.E056	SEG.RE.02	Alerta de espaço crítico para armazenamento das anotações dos eventos (*logs*)	**PR**: 1 - Verificar como é feito o controle do espaço de armazenamento das anotações de eventos(log); 2 - Verificar como são emitidos os alertas relacionados ao comprometimento do espaço de armazenamento. **RE**: O sistema DEVE suportar controle para o espaço de armazenamento e emitir alertas.
SEG.E057	SEG.RE.03	Integridade das trilhas de auditoria	**PR:** Verificar se as trilhas de auditorias podem ser alteradas, removidas ou substituídas total ou parcialmente pelos usuários com os seguintes papéis: AuditorTI, Atendente, e Corregedor. **RE:** Nenhum usuário deve poder conseguir alterar, remover ou substituir total ou parcialmente o conteúdo das trilhas de auditoria.
SEG.E058	SEG.RE.04	Eventos anotados	**PR:** A partir de um usuário com papel "AuditorTI", verificar a existência dos eventos: • Operações privilegiadas; • Criação e modificação de registros eletrônicos • Atividades de gerenciamento do ciclo de vida dos usuários e perfis; • Delegação de privilégio; • Exportação e importação de registros eletrônicos; • Exportação de registros de auditoria; • Acesso aos registros de auditoria; • Iniciação e encerramento do sistema • Tentativa de autenticação de usuário e seu resultado (sucesso ou falha); • Expiração e bloqueio do identificador do usuário; • Execução de atividades de verificação de integridade dos registros eletrônicos e seus resultados; • Realização de assinatura digital. **RE**: As anotações de eventos devem conter, no mínimo, os eventos relacionados acima.

ID	Ref	Requisito	Descrição
SEG.E059	SEG.RE.04	Conteúdo da anotação de evento (log)	**PR:** A partir de um usuário com papel "AuditorTI", verificar se as anotações de eventos contém as seguintes informações: • Instante de ocorrência (data e hora); • Descrição do evento; • Nível de criticidade; • Identificação do componente, terminal e usuário associado. **RE:** As anotações de eventos (logs) DEVEM conter, no mínimo, as seguintes informações.
SEG.E060	SEG.RE.05	Interface para visualização das anotações de eventos	**PR:** 1) Acessar o SREI com o usuário com papel "AuditorTI": a.Verificar se o sistema possui uma interface para a visualização das anotações de eventos (logs); b.Verificar se as anotações estão em ordem cronológica; 2) Acessar o SREI com o usuário com papel de "Atendente": a. Acessar a interface de visualização de das anotações de eventos. **RE**: O item 1 DEVE ser atendido com sucesso. O item 2 não DEVE ser atendido, somente o usuário com autorização pode ter acesso a interface de visualização as anotações de eventos.
SEG.E061	SEG.RE.06	Exportação dos registros de auditoria	**PR**: Acessar o SREI com o usuário que possui o papel de auditor: 1) Exportar os dados de auditoria para arquivo 2) Abrir o arquivo com programa especifico para criar/manipular planilhas eletrônicas. **RE**: Todas as atividades DEVEM ser realizadas com sucesso.

2.1.9 Tempo

ID	Ref	Requisito	Descrição
SEG.E062	SEG.T.01	Formato da representação de tempo (data e hora)	**PR**: Para todos os testes relacionados a anotações de eventos verificar a representação do instante de tempo (data e hora). **RE**: Todos os registros de instante de tempo devem indicar a data e hora mais a referência ao UTC com indicação do fuso local.
SEG.E063	SEG.T.02	Fonte de sincronismo de tempo	**PR**: Verificar se todo registro de tempo utiliza uma única e confiável fonte temporal. Verificar através de um usuário sem privilégios de administrador se é possível acessar a configuração da fonte temporal. **RE**: Todo registro deve utilizar uma única e confiável fonte temporal, e nenhum usuário deve ter acesso à configuração desta fonte temporal, somente o administrador.

2.1.10 Notificação de ocorrências

ID	Ref	Requisito	Descrição
SEG.E064	SEG.NO.01	Notificação de ocorrências	**PR**: Acessar o SREI com o usuário que possui o papel de “Escrevente” e na interface apropriada para notificação de ocorrência, inserir melhoramentos e sugestões para o sistema. **RE**: O SREI deve permitir a inserção de ocorrência: eventos críticos, problemas de

			segurança, problema de funcionamento do sistema, melhoramentos e sugestões.
SEG.E065	SEG.NO.02	Visualização das notificações de ocorrências	**PR**: Acessar o SREI com o usuário com papel de AdministradorTI e verificar se é possível visualizar as notificações de ocorrência. **RE**: O sistema DEVE fornecer uma interface para visualização das notificações de ocorrências.
SEG.E066	SEG.NO.03	Encaminhamento das notificações	**PR**: Verificar se o SREI armazena uma lista de e-mail para encaminhamento das ocorrências. **RE**: O SREI deve permitir a configuração de uma lista de e-mail.

2.1.11 Documentação do software SREI

ID	Ref	Requisito	Descrição
SEG.E067	SEG.DOC.01	Manuais do sistema	**PR:** Verificar se as seguintes documentações acompanham o SREI: • Instalação do sistema; • Configuração do sistema; • Uso do sistema; **RE**: O SREI deve acompanhar todas as documentações e recomendações citadas acima.
SEG.E068	SEG.DOC.02	Referência à versão do software	**PR:** Verificar no início de cada documento o versionamento. **RE:** Todos os documentos devem possuir versão.
SEG.E069	SEG.DOC.03	Manual de instalação e configuração do	**PR:** Verificar se os manuais voltados à instalação e configuração do sistema contêm as seguinte informações: • Visão geral do sistema;

		sistema	• Instalação e configuração do sistema; • Instalação e configuração dos componentes complementares ; • Recomendação sobre a forma de configuração segura do sistema; • Descrição dos perfis de usuários do sistema. **RE**: O manual de instalação e configuração do sistema deve conter minimamente as informações acima.
SEG.E069	SEG.DOC.04	Configuração do SGBD	**PR**: Verificar no manual de configuração se estão contemplados os tópicos referentes ao SGBD, incluindo controle de acesso. **RE**: O manual deve contemplar tópicos de instalação e configuração do SGBD, considerando as restrições de acesso a entidades não autorizadas.
SEG.E070	SEG.DOC.06	Operador de backup	**PR**: Verificar no manual de configuração se estão descritas as operações relativas ao usuário com o papel de operador de backup no SGBD. **RE**: O manual de configuração deve descrever quais atribuições do operador de backup e como configurá-las.

3 Referências bibliográficas

ICP-Brasil, 2007 — ICP-Brasil. **Manual de Condutas Técnicas 5 (MCT 5) Materiais e documentos técnicos para homologação de softwares de autenticação no âmbito da ICP-Brasil – Volume I: Requisitos**. ICP-Brasil. Versão 2.0. 2007.

SBIS, 2009a — SBIS. **Manual de Certificação para Sistemas de Registros Eletrônicos de Saúde (SRES).** Sociedade Brasileira de Informática em Saúde (SBIS) e Conselho Federal de Medicina (CFM). Versão 3.3. São Paulo. 2009.

SBIS, 2009b — SBIS. **Manual de Operacional de Ensaios e Análises para Sistemas de Registros Eletrônicos de Saúde (SRES).** Sociedade Brasileira de Informática em Saúde (SBIS) e Conselho Federal de Medicina (CFM). Versão 1.2. São Paulo. 2009.

ISO, 2007 — ABNT. **NBR ISO/IEC 27002: Tecnologia da Informação – Técnicas de segurança- Código de prática para gestão da segurança da informação**. Associação Brasileira de Normas Técnicas (ABNT). Rio de Janeiro. 2007.

OWASP, 2008 — OWASP. **Open Web Application Security Project Owasp Testing Guide**. Version 3.0. 2008.