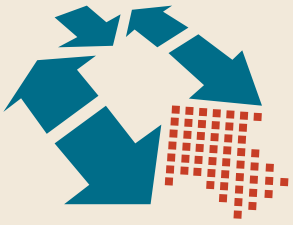

PADRÃO **TISS**

segurança & **privacidade**

Dezembro 2017

ANS Agência Nacional de Saúde Suplementar

Requisitos de segurança e privacidade do padrão TISS - Dezembro de 2017

Numeração	Descrição	Condição de utilização	Início de vigência	Fim de vigência	Data fim de implantação	OBS
1	Identificar e autenticar todo usuário antes de qualquer acesso a dados com identificação do beneficiário.	Obrigatório	out/12		ago/14	
2	Utilizar para autenticação de usuários a site e páginas da Internet (portais) login e senha podendo opcionalmente, desde que acordado entre as partes, ser utilizada a certificação digital.	Obrigatório	out/12		ago/14	
3	Utilizar para autenticação de usuários, via utilização de webservices, login e senha podendo opcionalmente, desde que acordado entre as partes, ser utilizada a certificação digital em substituição ao login e senha.	Obrigatório	out/12		ago/14	
4	Verificar a qualidade de segurança da senha no momento de sua definição pelo usuário obrigando a utilização de, no mínimo, 8 caracteres dos quais, no mínimo, 1 caractere deve ser não alfabético	Obrigatório	out/12		ago/14	
5	Definir o período máximo de troca de senha como controle do sistema. Este período não deve ser superior a um ano. O sistema deve permitir que o usuário troque sua senha a qualquer momento.	Obrigatório	out/12		ago/14	
6	Armazenar a senha dos usuários utilizando qualquer algoritmo HASH.	Obrigatório	out/12	dez/18	ago/14	Contido no item 39
7	Bloquear, ao menos temporariamente, o usuário após um número máximo de tentativas inválidas de login, por qualquer meio de acesso. Este número de tentativas não deve ser superior a cinco.	Obrigatório	out/12		ago/14	
8	Possuir controles de segurança na sessão de comunicação a fim de não permitir o roubo de sessão do usuário	Obrigatório	out/12	dez/18	ago/14	Contido no item 34
9	Oferecer os seguintes serviços de segurança na sessão de comunicação entre o componente cliente e o componente servidor: autenticação do servidor, integridade dos dados e confidencialidade dos dados.	Obrigatório	out/12	dez/18	ago/14	Contido no item 46
10	Encerrar a sessão do usuário após período de tempo configurável de inatividade. Este tempo não deve ser superior a trinta minutos.	Obrigatório	out/12	dez/18	ago/14	Contido no item 33
11	Registrar log de acessos e de tentativas de acesso ao sistema de informação.	Obrigatório	out/12		ago/14	
12	Utilizar certificado digital sempre dentro do período de validade além de não aceitar o certificado se o mesmo estiver na lista de certificados revogados da AC.	Obrigatório	out/12		ago/14	
13	Utilizar certificado digital que identifique o endereço eletrônico para o qual foi emitido	Obrigatório	out/12		ago/14	

Numeração	Descrição	Condição de utilização	Início de vigência	Fim de vigência	Data fim de implantação	OBS
14	Utilizar certificado digital que contemple em sua estrutura a identificação da autoridade certificadora emissora.	Obrigatório	out/12		ago/14	
15	Utilizar certificado digital que contemple em sua estrutura a identificação do titular do certificado	Obrigatório	out/12		ago/14	
16	Utilizar certificado digital que utilize protocolo criptográfico SSL ou TLS	Obrigatório	out/12		ago/14	
17	Utilizar certificado digital que utilize criptografia de, no mínimo, 128 bits	Obrigatório	out/12	dez/18	ago/14	Será substituido pelo item 35
18	Utilizar certificado digital que implemente autenticação por algoritmo HASH	Obrigatório	out/12		ago/14	
19	A interrupção do serviço de troca eletrônica de informações entre prestadores de serviços de saúde e operadoras de planos privados de assistência à saúde deve ser solucionada em até 48 (quarenta e oito) horas, salvo em caso fortuito ou de força maior devidamente justificado.	Obrigatório	out/12		ago/14	
20	Para as transmissões remotas de dados identificados, os sistemas das operadoras de planos de saúde deverão possuir um certificado digital de aplicação única emitido por uma Autoridade Certificadora.	Obrigatório	out/12	dez/18	ago/14	Será substituido pelo item 52
21	As operadoras de planos privados de assistência à saúde devem constituir proteções administrativas, técnicas e físicas para impedir o acesso eletrônico ou manual impróprio à informação de saúde, em especial à toda informação identificada individualmente.	Obrigatório	out/12		ago/14	
22	Deve conter a assinatura digital do prestador de serviços na guia de cobrança de internações para assegurar a autenticidade e o não repúdio das informações ali contidas	Opcional	out/12	dez/17		
23	Deve conter a assinatura digital do prestador de serviços na guia de cobrança de SP/SADT para assegurar a autenticidade e o não repúdio das informações ali contidas	Opcional	out/12	dez/17		
24	Deve conter a assinatura digital do prestador de serviços na guia de cobrança de consultas para assegurar a autenticidade e o não repúdio das informações ali contidas	Opcional	out/12	dez/17		
25	Deve conter a assinatura digital do prestador de serviços na guia de cobrança de serviços de odontologia para assegurar a autenticidade e o não repúdio das informações ali contidas	Opcional	out/12	dez/17		

Numeração	Descrição	Condição de utilização	Início de vigência	Fim de vigência	Data fim de implantação	OBS
26	Os prestadores de serviços de saúde devem constituir proteções administrativas, técnicas e físicas para impedir acesso impróprio à informação de saúde, eletrônico ou manual, em especial a toda informação identificada individualmente.	Obrigatório	jan/18		dez/18	Alterada a Condição de utilização
27	Seguir os itens de segurança descritos na Cartilha Sobre Prontuário Eletrônico para sistemas de registro saúde construída através de convênio, entre o CFM e a SBIS.eletrônico de	Recomendado	out/12	dez/17		
28	Observar a Resolução CFO-91/2009 que aprova as normas técnicas concernentes à digitalização, uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, quanto aos Requisitos de Segurança em Documentos Eletrônicos em Saúde.	Recomendado	out/12	dez/17		
29	Observar a RESOLUÇÃO CFM Nº 1.821/07 que aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde.	Recomendado	out/12	dez/17		
30	Deve conter a assinatura digital do prestador de serviços na mensagem enviada à operadora para assegurar a autenticidade, o não repúdio, a integridade e a garantia de origem.	Recomendado	jan/18			Alterada a Condição de utilização
31	Deve conter a assinatura digital da operadora na mensagem enviada ao prestador de serviços para assegurar a autenticidade e o não repúdio das informações ali contidas	Recomendado	jan/18			Alterada a Condição de utilização
32	Igualdade de senha: os processos de troca de senha devem exigir que a nova senha seja diferente da imediatamente anterior àquela já utilizada pelo usuário.	Obrigatório	jan/18		dez/18	
33	a) A sessão de usuário deve ser automaticamente bloqueada ou encerrada forçadamente pelo aplicativo após um período de inatividade.Este tempo não deve ser superior a 30 minutos. b) Após o bloqueio ou encerramento da sessão de usuário, as informações em tela não deverão mais estar visíveis, sendo necessária uma nova autenticação para a retomada da atividade. c) Não deve ser possível para qualquer usuário do sistema desativar ou desabilitar tais controles.	Obrigatório	jan/18		dez/18	

Numeração	Descrição	Condição de utilização	Início de vigência	Fim de vigência	Data fim de implantação	OBS
34	A sessão de comunicação remota entre cliente e servidor deve possuir controles de segurança que impeçam o roubo ou reuso da sessão do usuário. a) As credenciais de acesso não devem ser transmitidas entre as partes na forma de texto claro. b) Devem haver controles que impeçam o reuso de identificadores de sessão do usuário (por exemplo: ataques de replay e covert-channel) e roubo da sessão. c) Não deve ser possível para qualquer usuário do sistema desativar ou desabilitar tais controles.	Obrigatório	jan/18		dez/18	
35	Utilizar certificado digital que utilize criptografia de, no mínimo, 256 bits.	Obrigatório	jan/18		dez/18	
36	O sistema deve apresentar minimamente as informações de identificação do software, contendo obrigatoriamente o nome do software, nome do fornecedor, identificação completa da versão e/ou release e/ou build. Essas informações deverão estar disponíveis minimamente: • na tela inicial do sistema; • nas telas de cada módulo de modo que quando o sistema esteja em uso essas informações estejam sempre visíveis; • impressões geradas oriundas do sistema.	Obrigatório	jan/18		dez/18	
37	Todo usuário do sistema deve ser identificado e autenticado antes de qualquer acesso a dados ou funcionalidades do sistema.	Obrigatório	jan/18		dez/18	
38	Utilizar, nos processos de autenticação de usuário para acesso aos sistemas, um dos seguintes métodos: • Identificação de usuário e senha secreta de acesso; • Certificado digital; • Validação biométrica; • OTP.	Obrigatório	jan/18		dez/18	

Numeração	Descrição	Condição de utilização	Início de vigência	Fim de vigência	Data fim de implantação	OBS
39	Armazenar de forma protegida todos os dados ou parâmetros utilizados no processo de autenticação de usuário. Método: Nome de usuário e senha a) A senha deve ser armazenada em banco de dados, de forma codificada por algoritmo de hash aberto (público) de no mínimo 160 bits. b) As codificações das senhas de acesso dos usuários devem ser protegidas contra acesso não autorizado. Método: Biometria (condição: somente para pessoas) c) Os templates biométricos das pessoas devem ser protegidos contra acesso não autorizado. Apenas o usuário do banco de dados utilizado pela aplicação deve ter acesso aos mesmos. d) As amostras biométricas coletadas e transmitidas durante o processo de autenticação devem ser protegidas contra acesso não autorizado. Método: One-time password (OTP) e) As sementes de geração dos valores numéricos devem ser protegidas contra acesso não autorizado. Apenas o usuário do banco de dados utilizado pela aplicação deve ter acesso aos mesmos.	Obrigatório	jan/18		dez/18	
40	a) O sistema deve possuir, em todos os processos de autenticação de usuário, independentemente do método de autenticação utilizado, mecanismos para bloquear a conta deste usuário no sistema após um número máximo configurável de tentativas consecutivas de login com autenticação inválida, que não exceda a 05 (cinco) tentativas. b) Após o bloqueio de conta de um usuário, o sistema só deve permitir login deste após o desbloqueio de sua conta de usuário.	Obrigatório	jan/18		dez/18	

Numeração	Descrição	Condição de utilização	Início de vigência	Fim de vigência	Data fim de implantação	OBS
41	a)Identidade única: toda pessoa usuária do sistema deverá ser identificada individualmente. b)Vinculação a número legal e único: toda pessoa usuária do sistema deverá ser vinculada minimamente a um documento de identificação pessoal unívoco. c)Unicidade de identificação de usuários: a informação de identificação de tal documento deverá ser validada na inclusão ou alteração de pessoas para garantir a unicidade, ou seja,o sistema não deve permitir a associação de um mesmo documento de identificação a dois usuários no sistema. d)Exclusão de usuários: Para fins de responsabilização, não deve ser possível remover o cadastro ou vínculo de usuários e profissionais de saúde do sistema, caso alguma operação tenha sido realizada pelo mesmo. Que seja possível inativar usuário, apesar de não poder excluir, e que o inativo não consiga fazer login/acessar.	Obrigatório	jan/18		dez/18	
42	Assim que completada uma autenticação com sucesso,o sistema deve exibir à pessoa usuária as seguintes informações: • Data e hora da última autenticação com sucesso de seu usuário; • Data e hora das tentativas de autenticação sem sucesso depois da última autenticação com sucesso. Nota: Considera-se como “última autenticação” a autenticação anterior à que está ocorrendo.	Obrigatório	jan/18		dez/18	
43	Condição: Arquitetura cliente-servidor e autenticação por login e senha. A interface de usuário utilizada para digitação de credenciais de acesso ao sistema (login ou nome do usuário, senha secreta de acesso, PIN) deve impedir a memorização e a visualização de dados anteriores (lista de logins já digitados, lembrança automática de senhas associadas a um login, etc.). Além disso, toda e qualquer digitação direta de senhas deve ser feita por meio de máscara de caracteres que impeça sua visualização por outras pessoas.	Obrigatório	jan/18		dez/18	
44	Impedir acesso ou visualização dos dados por pessoas não autorizadas no sistema.	Obrigatório	jan/18		dez/18	
45	Garantir que o acesso aos dados do sistema seja somente possível por meio de canais de interação pré-definidos (ex.: web, console local, interface entre aplicativos), com atuação obrigatória de mecanismos de controle de acesso.	Obrigatório	jan/18		dez/18	

Numeração	Descrição	Condição de utilização	Início de vigência	Fim de vigência	Data fim de implantação	OBS
46	a) A sessão de comunicação entre o componente de interação com o usuário (ex.: browser ou executável cliente) e os outros componentes do sistema (ex.: servidor de aplicação, banco de dados, etc) deve oferecer os seguintes serviços de segurança: autenticação do servidor, integridade dos dados e confidencialidade dos dados. b) O serviço de segurança empregado deve implementar criptografia dos dados em trânsito.	Obrigatório	jan/18		dez/18	
47	A comunicação entre componentes distribuídos (como, por exemplo, entre a aplicação e o banco de dados) deve oferecer os seguintes serviços de segurança: autenticação de parceiros (ambas as partes), integridade dos dados e confidencialidade dos dados (criptografia).	Obrigatório	jan/18		dez/18	
48	Dados estruturados devem ser armazenados por Sistema(s) de Gerenciamento de Banco de Dados (SGBD) e dados não estruturados e não armazenados em SGBD devem ser criptografados.	Obrigatório	jan/18		dez/18	
49	Os dados inseridos pelo usuário nos campos de entrada (inputs, caixas de texto, etc) devem ser validados antes de serem processados, de forma a prevenir ataques de buffer overflow e injeção de dados.	Obrigatório	jan/18		dez/18	
50	O sistema deve permitir o gerenciamento (criação, ativação/inativação e modificação) de usuários e papéis (perfis), por meio da aplicação, de forma a possibilitar o controle de acesso às funcionalidades do sistema conforme os papéis aos quais o usuário possui. Um usuário pode possuir um ou mais papéis.	Obrigatório	jan/18		dez/18	
51	Em caso de autenticação inválida em tentativa de acesso, a mensagem de erro emitida pelo sistema para o usuário não deve informar qual o motivo do erro.	Obrigatório	jan/18		dez/18	
52	Para as transmissões remotas de dados identificados, os sistemas das operadoras de planos de saúde deverão possuir um certificado digital de servidor emitido por uma Autoridade Certificadora. AC certificados de servidor homologada WebTrust for CAs, WebTrust for CAs - SSL Baseline with Network Security e WebTrust for CAs - EV SSL (se emitir EV), e ETSI TS 102 042, ETSI EN 319 411-1 e ETSI EN 319 411-2	Obrigatório	jan/18		dez/18	
53	Todos os processos de validação de dados devem ser realizados no lado do servidor. Opcionalmente, poderá haver validação de dados inicialmente no lado cliente desde que seguida de validação no lado do servidor.	Recomendado	jan/18			

Numeração	Descrição	Condição de utilização	Início de vigência	Fim de vigência	Data fim de implantação	OBS
54	O sistema deve ser composto por componentes distribuídos. O banco de dados deve estar distanciado do usuário de forma a dificultar ataques. Para isso, o banco de dados deve estar segregado em relação à aplicação física ou logicamente.	Recomendado	jan/18			
55	O acesso de usuários ao SGBD deve ser permitido somente por intermédio do componente de autenticação e controle de acesso com usuário exclusivo para esse fim, exceto nas atividades de cópia de segurança (suporte de maneira geral).	Recomendado	jan/18			
56	Componentes que manipulam dados identificados do sistema para fins de interoperabilidade, visualização, assinatura e outros, não devem manter tais dados fora do SGBD após o término da operação.	Recomendado	jan/18			
57	Gerar log de auditoria.	Recomendado	jan/18			
58	Os registros de auditoria gerados devem ser protegidos contra acesso não autorizado e contra qualquer tipo de alteração.	Recomendado	jan/18			
59	O sistema deve possuir uma interface para visualização dos registros de auditoria em ordem cronológica.	Recomendado	jan/18			
60	Toda pessoa usuária do sistema deve ter a autenticação confirmada no momento da realização de operações críticas ou sensíveis, mesmo que já tenha se autenticado previamente para ingresso ao sistema.	Recomendado	jan/18			
61	Condição: sistema permite a retomada da atividade após bloqueio de sessão de usuário por inatividade ou manualmente pelo usuário. O sistema deverá permitir a retomada da atividade dousuário após bloqueio de sessão. Essa operação é permitida apenas quando o desbloqueio for realizado pelo mesmo usuário bloqueado. Para que o desbloqueio de sessão seja realizado, o sistema deve requerer novo processo de autenticação do usuário bloqueado.	Recomendado	jan/18			
62	A base de dados que contém informações de saúde deve estar criptografada.	Recomendado	jan/18			

Ministério da
Saúde