

Requisitos de segurança e privacidade do padrão TISS vigentes no Padrão TISS - Julho de 2021

Escopo Os requisitos que compõem esta relação, se aplicam a todos os sistemas e portais que tratam os dados que fazem parte do Padrão TISS para troca de informações na saúde suplementar.



Numeração	Descrição	Condição de utilização	Início de vigência	Fim de Vigência	Data limite para 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	jul/22	ago/14	Será substituído pelo requisito 67
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	jul/22	ago/14	Será substituído pelo requisito 68
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	jul/22	ago/14	Será substituído pelo requisito 69
11	Registrar log de acessos e de tentativas de acesso ao sistema de informação.	Obrigatório	out/12	jul/22	ago/14	Será substituído pelo requisito 70
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	
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	jul/22	ago/14	Será substituído pelo requisito 71
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	jul/22	ago/14	Será substituído pelo requisito 72
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	jul/22	ago/14	Será substituído pelo requisito 73
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	out/12	jul/22	ago/14	Será substituído pelo requisito 74
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			
31	Deve conter a assinatura digital da operadora na mensagem enviada ao prestador de serviços para assegurar a autenticidade, a integridade do conteúdo e o não repúdio das informações ali contidas.	Recomendado	jan/18			
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	jul/22	dez/18	Será substituído pelo requisito 75

33	<p>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.</p> <p>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.</p> <p>c) Não deve ser possível para qualquer usuário do sistema desativar ou desabilitar tais controles.</p>	Obrigatório	jan/18	jul/22	dez/18	Será substituído pelo requisito 76
34	<p>A sessão de comunicação remota entre cliente e servidor deve possuir controles de segurança que impeçam o roubo ou reuso da sessão do usuário.</p> <p>a) As credenciais de acesso não devem ser transmitidas entre as partes na forma de texto claro.</p> <p>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.</p> <p>c) Não deve ser possível para qualquer usuário do sistema desativar ou desabilitar tais controles.</p>	Obrigatório	jan/18		dez/18	
35	Utilizar certificado digital que utilize criptografia de, no mínimo, 256 bits.	Obrigatório	jan/18		dez/18	
36	<p>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.</p> <p>Essas informações deverão estar disponíveis minimamente:</p> <ul style="list-style-type: none"> • na tela inicial do sistema; • nas telas de cada módulo de modo que quando o sistema esteja em uso essas informações estejam sempre visíveis; <p>Essas informações deverão estar disponíveis minimamente:</p>	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	<p>Utilizar, nos processos de autenticação de usuário para acesso aos sistemas, um dos seguintes métodos:</p> <ul style="list-style-type: none"> • Identificação de usuário e senha secreta de acesso; • Certificado digital; • Validação biométrica; • OTP. 	Obrigatório	jan/18		dez/18	
39	<p>Armazenar de forma protegida todos os dados ou parâmetros utilizados no processo de autenticação de usuário.</p> <p>Método: Nome de usuário e senha</p> <p>a) A senha deve ser armazenada em banco de dados, de forma codificada por algoritmo de hash aberto (público) de no mínimo 160 bits.</p> <p>b) As codificações das senhas de acesso dos usuários devem ser protegidas contra acesso não autorizado.</p> <p>Método: Biometria (condição: somente para pessoas)</p> <p>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.</p> <p>d) As amostras biométricas coletadas e transmitidas durante o processo de autenticação devem ser protegidas contra acesso não autorizado.</p> <p>Método: One-time password (OTP)</p> <p>e) As sementes de geração dos valores numéricos devem ser protegidas contra acesso não autorizado.</p> <p>Apenas o usuário do banco de dados utilizado pela aplicação deve ter acesso aos mesmos.</p>	Obrigatório	jan/18	jul/22	dez/18	Será substituído pelo requisito 77
40	<p>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.</p> <p>b) Após o bloqueio de conta de um usuário, o sistema só deve permitir login deste após o desbloqueio de sua conta de usuário.</p>	Obrigatório	jan/18	jul/21	dez/18	

41	<p>a)Identidade única: toda pessoa usuária do sistema deverá ser identificada individualmente.</p> <p>b)Vinculação a número legal e único: toda pessoa usuária do sistema deverá ser vinculada minimamente a um documento de identificação pessoal unívoco.</p> <p>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.</p> <p>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.</p>	Obrigatório	jan/18		dez/18	
42	<p>Assim que completada uma autenticação com sucesso,o sistema deve exibir à pessoa usuária as seguintes informações:</p> <ul style="list-style-type: none"> • 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. <p>Nota: Considera-se como “última autenticação” a autenticação anterior à que está ocorrendo.</p>	Obrigatório	jan/18		dez/18	
43	<p>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.</p>	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	
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	jul/22	dez/18	
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.: aplicação) deve oferecer os seguintes funcionalidades de segurança: autenticação, integridade dos dados e confidencialidade dos dados. b) O componente de segurança empregado deve implementar criptografia na comunicação utilizando algoritmo de, no mínimo, 256 bits.	Obrigatório	ago/21		jul/22	
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	jul/22	dez/18	Será substituído pelo requisito 78
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	jul/22	dez/18	Será substituído pelo requisito 79
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	jul/22	dez/18	Será substituído pelo requisito 80
53	Todos os processos de validação das regras de negócio (ex.: validação de dados, conteúdo, tamanho, domínio, etc.) devem ser realizados no back-end. Opcionalmente, poderá haver tais validações no front-end, desde que seguidas das validações no back-end.	Obrigatório	ago/21		jul/22	
54	A arquitetura do sistema deverá estar disposta em camadas e seus componentes distribuídos. O banco de dados deverá estar segregado das aplicações (ex.: componentes, segmentos de rede, API).	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 <u>segurança (suporte de maneira geral)</u> .	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.	Obrigatório	ago/21		jul/22	
57	Gerar trilhas de auditoria das ações realizadas no tratamento de dados pessoais e pessoais sensíveis.	Obrigatório	ago/21		jul/22	

58	Os registros de auditoria gerados devem ter garantia de integridade e serem protegidos contra acesso não autorizado.	Obrigatório	ago/21		jul/22	
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 do usuário 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	jul/22		
62	As bases de dados, mídias ou arquivos que contém dados pessoais e/ou dados pessoais sensíveis devem ser protegidas para garantir a confidencialidade (por exemplo: criptografia, somente acessos autorizados, etc.)	Obrigatório	ago/21		jul/22	
63	Utilização de captcha na tela de acesso ao sistema vinculada ao método de autenticação por login e senha. Não deve ser permitido autenticar o usuário sem a validação simultânea do login, senha e token do captcha.	Recomendado	ago/21			
64	Adotar a criptografia de, no mínimo, 256 bits na comunicação entre as partes da aplicação em redes distintas.	Recomendado	ago/21			
65	Utilização de captcha na tela de recuperação de senha de acesso do sistema para evitar ataques do tipo Brute Force	Recomendado	ago/21			
66	Não permitir alterar e remover registros do log de auditoria de sistema por um tempo mínimo de 90 dias	Obrigatório	ago/21		jul/22	

67	Mínimo de 08 caracteres utilizando pelo menos um (01) caractere de cada um dos quatro (4) tipos de caracteres listados abaixo: <ul style="list-style-type: none"> • Letras Maiúsculas (AZ) • Letras Minúsculas (az) • Números (0-9) 	Obrigatório	ago/21		jul/22	
68	Definir o período máximo de troca de senha como controle do sistema. Este período não deve ser superior a 180 (cento e oitenta dias). O sistema deve permitir que o usuário troque sua senha a qualquer momento.	Obrigatório	ago/21		jul/22	
69	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. Após o número máximo de tentativas, o usuário poderá ser bloqueado por, no mínimo, 5 (cinco) minutos ou ser submetido a outros controles para autenticação. O desbloqueio será feito apenas pelo próprio usuário ou a sessão será encerrada.	Obrigatório	ago/21		jul/22	
70	Registrar log de acessos e de tentativas de acesso ao sistema de informação. O tempo de armazenamento desta informação seja de, no mínimo, 90 (noventa) dias.	Obrigatório	ago/21		jul/22	
71	Utilizar certificado digital que utilize apenas protocolo criptográfico TLS na versão mínima 1.2.	Obrigatório	ago/21		jul/22	
72	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 corridas, salvo em caso fortuito ou de força maior devidamente justificado.	Obrigatório	ago/21		jul/22	
73	As operadoras de planos privados de assistência à saúde devem constituir proteções administrativas, técnicas e físicas para impedir o acesso não autorizado à dados pessoais e dados pessoais sensíveis.	Obrigatório	ago/21		jul/22	
74	Os prestadores de serviços de saúde devem constituir proteções administrativas, técnicas e físicas para impedir o acesso não autorizado à dados pessoais e dados pessoais sensíveis, em especial à toda informação identificada individualmente.	Obrigatório	ago/21		jul/22	

75	Igualdade de senha: os processos de troca de senha devem exigir que a nova senha seja diferente das três últimas senhas utilizadas pelo usuário.	Obrigatório	ago/21		jul/22	
76	<p>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.</p> <p>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.</p> <p>c) Não deve ser possível para qualquer usuário do sistema desativar ou desabilitar tais controles.</p> <p>d) Para que o desbloqueio de sessão seja realizado, o sistema deve requerer novo processo de autenticação do usuário bloqueado.</p>	Obrigatório	ago/21		jul/22	
77	<p>Armazenar de forma protegida todos os dados ou parâmetros utilizados no processo de autenticação de usuário.</p> <p>Método: Nome de usuário e senha</p> <p>a) A senha deve ser armazenada em banco de dados, de forma codificada por algoritmo criptográfico no mínimo igual a 256 bits.</p> <p>b) As codificações das senhas de acesso dos usuários devem ser protegidas contra acesso não autorizado.</p> <p>Método: Biometria (condição: somente para pessoas)</p> <p>c) Os templates biométricos das pessoas devem ser protegidos contra acesso não autorizado.</p> <p>d) As amostras biométricas coletadas e transmitidas durante o processo de autenticação devem ser protegidas contra acesso não autorizado.</p> <p>Método: OTP</p> <p>e) As sementes de geração dos valores devem ser protegidas contra acesso não autorizado.</p>	Obrigatório	ago/21		jul/22	

78	A comunicação entre componentes distribuídos do sistema (como por exemplo, entre a aplicação e o banco de dados) devem oferecer controles de segurança para impedir acesso não autorizado. Para tal, deverão ser utilizados componentes de segurança que garantam a autenticação e a confidencialidade entre as partes da aplicação e a integridade dos dados.	Obrigatório	ago/21		jul/22	
79	Dados pessoais e pessoais sensíveis estruturados devem ser armazenados por Sistema(s) de Gerenciamento de Banco de Dados (SGBD) e dados pessoais e pessoais sensíveis não estruturados e não armazenados em SGBD devem atender à requisitos de confidencialidade.	Obrigatório	ago/21		jul/22	
80	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 ETSI TS 102 042, ETSI EN 319 411-1 e ETSI EN 319 411-2 .	Obrigatório	ago/21		jul/22	