

PADRÃO TISS

Padrão de Segurança e Privacidade

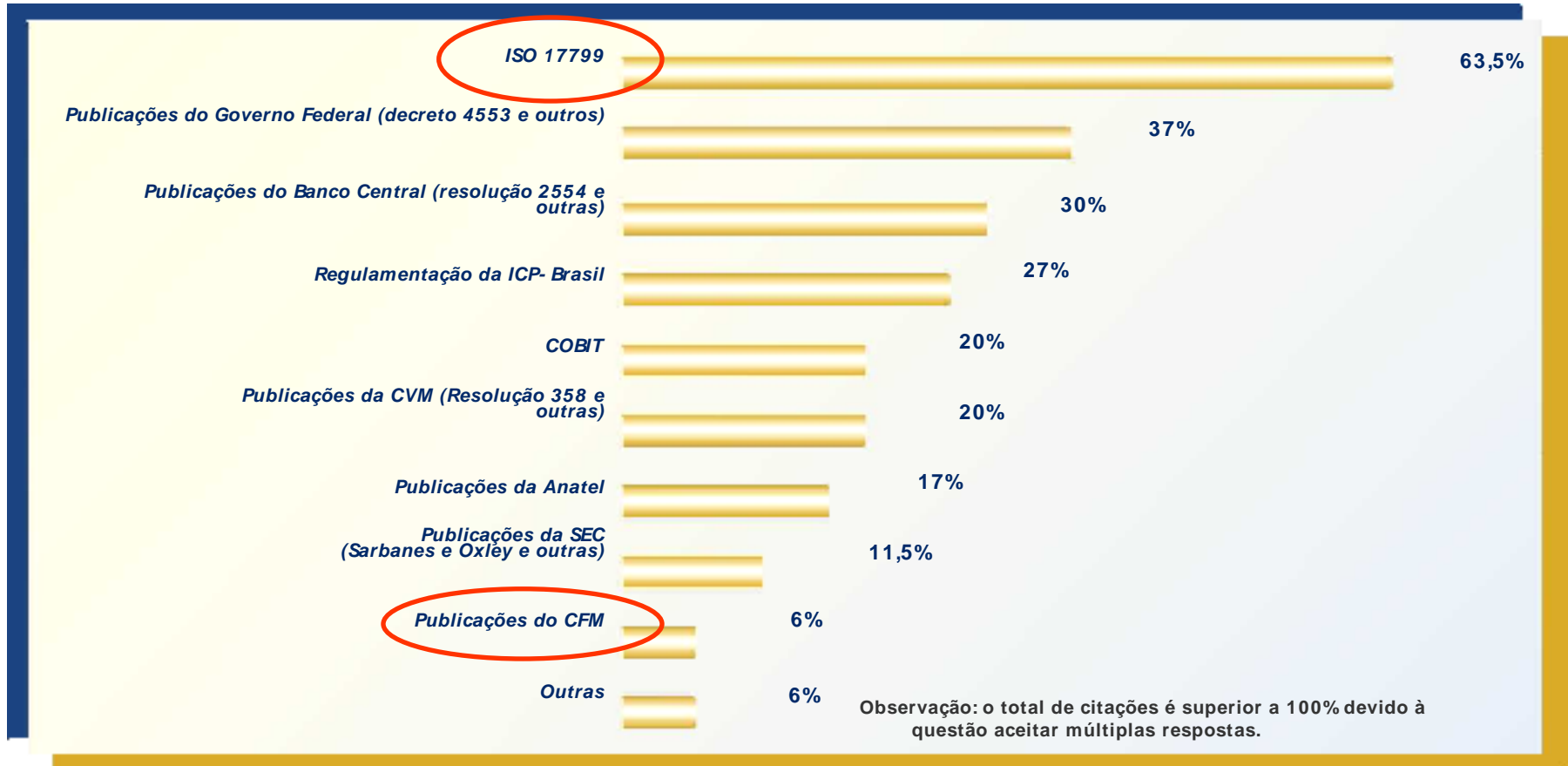
SEGURANÇA

RN nº 114/2005 – Artigo 8º
CAPÍTULO V
Da Segurança e da Privacidade

A Internet no Brasil

Pesquisa da Módulo Security (out-2003)

Legislações, normas e regulamentações de segurança que norteiam suas organizações



Pesquisa realizada com cerca de 50% das 1000 maiores empresas brasileiras- Financeiro (21%), Governo (17%), Indústria e Comércio (14%), Tecnologia/Informática (14%), Prestação de Serviços (9%), Outros (8%), Telecomunicações (7%), Comércio/Varejo (4%), Energia Elétrica (2%), Educação (2%) e Saúde (2%)

Resolução Normativa nº 114/2005 e Instrução Normativa/ DIDES nº 17/2005

- RN nº 114 /2005: estabelece o padrão TISS
 - Guias e demonstrativos de retorno;
 - Transações eletrônicas;
 - Cronograma;
 - COPISS;
 - Requisição de informações pela ANS,
 - Segurança e privacidade;**
 - Penalidades
- IN nº 17/2005: estrutura física do padrão
 - Anexo I: lay-out das guias e demonstrativos
 - Anexo II: transações eletrônicas
 - Anexo III: XML

Segurança e privacidade

- **CFM – Resolução 1638/2002**

Prontuário Médico: documento único constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo

- **CFM – Resolução 1639/2002**

“Normas Técnicas para uso dos sistemas informatizados para a guarda e manuseio do prontuário médico”

- **Constituição Federal**

– art. 5º “São invioláveis a intimidade, a honra,.....”

Segurança e privacidade

- RN 114/2005 – Artigo 8º

Proteção à informação identificada individualmente:

- CFM nº 1639/2002 e ANS–RN nº 21/2002 e ANS–RDC nº 64/2001
- recomenda o uso do manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES) – ISO 17799 – www.sbis.org.br ou www.cfm.org.br

IN nº 17/2005 – Anexo II – define **HASH MD5** no epílogo da mensagem

Segurança e privacidade

- **Agência Nacional de Saúde Suplementar**

Resolução RDC nº 64 de 10/04/2001

- *“Dispõe sobre a designação de médico responsável pelo fluxo de informações relativas à assistência médica prestada aos consumidores de planos privados de assistência à saúde.”*

Resolução RN nº 21 de 12/12/2002

- *“Art. 1º As operadoras de planos privados de assistência à saúde deverão manter protegidas as informações assistenciais fornecidas pelos seus consumidores ou por sua rede de prestadores, observado o disposto na Resolução – RDC nº 64, de 10 de abril de 2001, quando acompanhadas de dados que possibilitem a sua individualização, não podendo as mesmas ser divulgadas ou fornecidas a terceiros, salvo em casos expressamente previstos na legislação.”*

Segurança e privacidade

- **RN 124 de 03/04/2006** – Dispõe sobre a aplicação de penalidades para as infrações à legislação dos planos privados de assistência à saúde.

“Informação sobre Condições de Saúde dos Consumidores

Art. 72. Divulgar ou fornecer a terceiros não envolvidos na prestação de serviços assistenciais, informação sobre as condições de saúde dos consumidores, contendo dados de identificação, sem a anuência expressa dos mesmos, salvo em casos autorizados pela legislação:

Sanção – multa de R\$ 50.000,00....”.

“Proteção de Informação sobre Consumidor

Art. 73. Deixar de adotar os mecanismos mínimos de proteção à informação em saúde suplementar, previstos na regulamentação da ANS:

Sanção – multa de R\$ 50.000,00.

Parágrafo único. Na hipótese de reincidência,...”

Segurança e privacidade

- **RN 114/2005** – Não estabelece padrões de segurança próprios do TISS

Art 8º “As operadoras de plano privado de assistência à saúde e prestadores de serviços de saúde devem constituir proteções administrativas, técnicas, e físicas para impedir o acesso eletrônico ou manual impróprio à informação de saúde, em especial a toda informação identificada individualmente, conforme normas técnicas estabelecidas na Resolução CFM nº 1639 de 10 de julho de 2002, e na RN nº 21 de 12 de dezembro de 2002, e na RDC nº 64 de 10 de abril de 2001 ambas da ANS.”

Parágrafo único. “Para que os objetivos de segurança e privacidade sejam alcançados, recomenda-se que sejam observados pelo menos os requisitos de segurança do Nível de Garantia de Segurança 1 (NGS-1), descritos no Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES) publicado na página da Sociedade Brasileira de Informação em Saúde – SBIS e do Conselho Federal de Medicina – CFM, conforme norma NBR ISO/IEC 17799 – Código de Prática para a Gestão da Segurança da Informação.”

Segurança e privacidade

- Manual de **Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES)**
- Base teórica: Comitê ISO 215 – Informática em Saúde

Registro Eletrônico em Saúde (RES): *padronização na área de informação em saúde e tecnologia da informação com o objetivo de atingir a compatibilidade e a interoperabilidade entre sistemas independentes. Garantir a compatibilidade de dados para fins de análise estatística, reduzindo redundâncias e a duplicação de esforços.*

Segurança e privacidade

- Com a troca eletrônica os problemas de segurança e privacidade se multiplicam
- Uma das funções do intercâmbio eletrônico de dados (EDI) é permitir a aplicação de **mecanismos de segurança**

Confidencialidade: criptografia (garante que a mensagem eletrônica trocada seja pelas partes realmente envolvidas)

Autenticação: uso de senhas, certificados digitais (as partes envolvidas devem estar “confiantes”)

Integridade dos dados: uso de algoritmos para garantir que os dados não sejam modificados na transação

Aceitação da mensagem: assinatura digital (nenhuma parte envolvida pode negar a transação)

Segurança e privacidade

- Manual de **Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES): NBR ISO 17799 e ISO 15408**

NBR ISO/IEC 17799: versão brasileira da ISO/IEC 17799 –

parte 1: código de práticas (*best practices*)

parte 2: orientações para a criação de Sistemas de Gestão de Segurança

ISO/IEC 15408: *Evaluation criteria for IT Security* : auxilia o desenvolvedor de *software* a incluir, melhorar ou simplesmente avaliar os aspectos de segurança do software em desenvolvimento

Segurança e privacidade

- Infra-estrutura de ICP-Brasil: chaves públicas brasileiras (MP nº 2200 de agosto de 2001 www.icpbrasil.com.br)
- Marco importante: valida os documentos eletrônicos
- Certificados digitais: garante a segurança de sistemas de informação, confirmando a identidade de seus usuários, servidores e processos.
- Certificados são pares de chaves formados por uma chave pública e uma chave privada
- Informação criptografada com a chave pública de um usuário só pode ser aberta com a chave privada correspondente e vice-versa
- Chave pública é disponibilizada e a chave privada é mantida em segredo pelo usuário

Segurança e privacidade

- **Níveis de segurança 1- NGS1** – assinatura manual – 11 requisitos

Requisito 1: controle de versão do software

Requisito 2: autenticação e controle de acesso – mecanismos de administração de usuários ligados a administrador do sistema – controles de acesso, perfis, grupos, senhas, perfil para execução de backup, permitir somente a inclusão de dados

Requisito 3: acesso aos dados do paciente com controle

Requisito 4: mecanismos de certificação de origem que garantam que somente informações oriundas de servidores internos sejam aceitas por estações clientes e vice-versa

Requisito 5: controle de sigilo e integridade – acessos

Requisito 6: cópias de segurança e restauração de dados: canal seguro para troca de informação e backup

Segurança e privacidade

- **Níveis de segurança 1- NGS1** – assinatura manual

Requisito 7: canais seguros de comunicação para sistemas baseados em arquitetura client-server e WEB: técnicas de criptografia, https

Requisito 8: utilização de recursos computacionais – requisitos para falhas de hardware e software

Requisito 9: Auditoria – trilhas de auditoria que garantam integridade e confidencialidade

Requisito 10: cópias de segurança e restauração de dados

Requisito 11: documentação

Segurança e privacidade

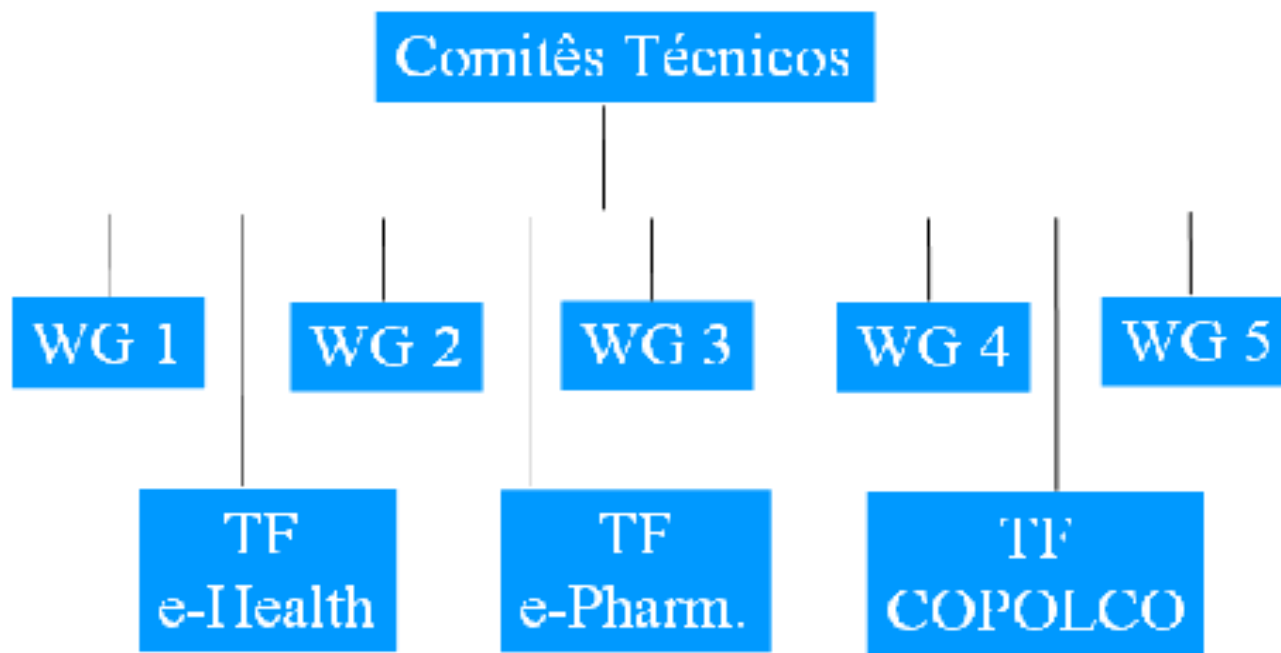
- **Níveis de segurança 2- NGS2** – certificados digitais em processos de autenticação, ou seja, baseados em assinatura digital

Requisito 1: origem de certificados digitais – de acordo com a MP 2200 de 2001

Requisito 2: controle de autenticação pelo uso de certificados digitais – assinatura digital

Comitês Técnicos da ISO TC215

Informática em Saúde



WG1 – Modelos de Registro Eletrônico

WG2 – Mensagens e Comunicação

WG3 – Representação de Conceitos em Saúde

WG4 – Segurança

WG5- Cartões em Saúde




International Organization for Standardization

- Home
- Site map
- Abbreviations
- ISO Store
- Français
- FAC
- Contact ISO
- My account

Search: All ? [Expanded Search](#)

- About ISO
- Products and services
- ISO 2000 / 21000
- Standards development
- Communities of interest
- Communication centre



ISO/IEC 19796-1:2005
benchmarks the quality of e-learning.

Standards development

- [Who does what, when and how?](#)
- [Technical committees](#)
 - General information
 - [List of technical committees](#)
 - [Other bodies developing standards or guides](#)
- [Business plans for public review](#)
- [ISO technical programme](#)
- [Participation in the technical work](#)
- [International organisations in liaison with technical committees](#)

TC 215

- Health informatics
- Secretariat
- Secretary
- Chair
- Scope

[ANSI](#)

Mr. Audrey T. Jensen
Dr. Yun Suk Kwak (Korea) until end 2005

Standardization in the field of information for health, and Health Information and Communications Technology (ICT) to achieve compatibility and interoperability between independent systems. Also, to ensure compatibility of data for comparative statistical purposes (e.g. classification), and to reduce duplication of effort and redundancies.

Total number of published ISO standards related to the TC and its SC: [29](#)
Number of published ISO standards under:



- [standards development](#)
- [Who does what, when and how?](#)
- [Technical committees](#)
- [General information](#)
- [List of technical committees](#)
- [Other bodies developing standards or guides](#)
- [Business plans for public review](#)
- [ISO technical programs](#)
- [Participation in the technical work](#)
- [International organizations in liaison with technical committees](#)
- [Meeting calendar](#)
- [For standards developers](#)

TC 215

Health informatics

Secretariat: [ANSI](#)
 Secretary: Ms Audrey Dickinson
 Chair: Dr. Yoo Suk Kwak (Korea) until end 2009
 Scope:

Standardization in the field of information for health, and Health Information and Communications Technology (ICT) to achieve compatibility and interoperability between independent systems. Also, to ensure compatibility of data for comparative statistical purposes (e.g. classifications), and to reduce duplication of effort and redundancies.

Total number of published ISO standards related to the TC and its SCs: [32](#)

Number of published ISO standards under the direct responsibility of the TC 215

Secretariat: [32](#)

Participating countries: [26](#)

Observer countries: [15](#)

Other ISO and IEC committees in liaison: [ISO TC 37](#), [TC 42](#), [TC 46](#), [TC 76](#), [TC 84](#), [TC 106](#), [TC 121](#), [TC 150](#), [TC 154](#), [TC 168](#), [TC 170](#), [TC 171](#), [TC 172](#), [TC 194](#), [TC 198](#), [TC 210](#), [TC 212](#), [TC 229](#), [ISO/IEC JTC 1/SC 2](#), [JTC 1/SC 6](#), [JTC 1/SC 7](#), [JTC 1/SC 22](#), [JTC 1/SC 23](#), [JTC 1/SC 24](#), [JTC 1/SC 27](#), [JTC 1/SC 32](#), [JTC 1/SC 37](#), [ISO/IEC JTC 1/SC 42](#), [ISO/IEC JTC 1/SC 43](#)



Países participantes do Comitê ISO/TC215

Secretariat:

USA (ANSI)

Participating countries:

Australia (SA)

Austria (ON)

Belgium (IBN)

Canada (SCC)

Czech Republic (CNI)

Denmark (DS)

Finland (SFS)

France (AFNOR)

Germany (DIN)

Israel (SII)

Italy (UNI)

Japan (JISC)

Kenya (KEBS)

Korea, Republic of (KATS)

Netherlands (NEN)

New Zealand (SNZ)

Norway (SN)

Russian Federation (GOST R)

Serbia and Montenegro (ISSM)

South Africa (SABS)

Spain (AENOR)

Sweden (SIS)

Turkey (TSE)

United Kingdom (BSI)

Observer countries:

Argentina (IRAM)

China (SAC)

Croatia (HZN)

Ecuador (INEN)

Hungary (MSZT)

India (BIS)

Iran, Islamic Republic of (ISIRI)

Ireland (NSAI)

Mongolia (MASM)

Poland (PKN)

Portugal (IPQ)

Singapore (SPRING SG)

Switzerland (SNV)

Thailand (TISI)

Zimbabwe (SAZ)

Prazos

- Prazo para o padrão de conteúdo e estrutura:
 - guias médicas – 30 de novembro de 2006
 - guias odontológicas – 31 de maio de 2007

- Prazos diferenciados para a troca eletrônica:
operadoras x grupos de prestadores
 - Grupo I: hospitais e clínicas – 31 de maio de 2007
 - Grupo II: consultórios médicos e odontológicos – 30 de novembro de 2008
 - Grupo III: clínicas odontológicas – 30 de novembro de 2007

Em aprovação pela Colegiada

Macro objetivos

- Permitir para todos os *stakeholders*:

Avaliação da Assistência à Saúde (caráter clínico, epidemiológico e administrativo)

Planejamento do setor

Interoperabilidade

Indicadores (sócio demográficos, morbidade, mortalidade, oferta e utilização de serviços, coberturas)

Benefícios

- Faturamento padronizado: redução de custos e otimização do uso dos recursos de tecnologia da informação e dos recursos humanos
- Redução do tempo consumido com transações em papel/telefone/fax
- Recursos focalizados nos processos de exceção, não na rotina
- Redução do re-trabalho
- Aprimoramento do processo de pagamento : redução de glosas, dados insuficientes ou inadequados para o processo de autorização
- Otimização do prazo de recebimento

Simplificação Administrativa!

