CEE78IS
Comissão de Estudo Especial
de Informática em Saúde

Associação Brasileira de Normas Técnicas (ABNT)

Comissão de Estudo Especial de Informática em Saúde (CEE78-IS)

GT4 – Segurança da Informação e do Paciente

8ª Plenária CEE78IS – 15/09/2015

CEE78IS

Comissão de Estudo Especial de Informática em Saúde

APRESENTAÇÃO DO PROJETO DE NORMA Nº: 078:000.000-078

Objetivo do trabalho: Adoção no Brasil da norma ISO 27799:2008 - Health informatics - Information security management in health using ISO/IEC 27002

Nome da versão brasileira:

ABNT NBR XX ISO 27799 - Informática em saúde — Gestão de segurança da informação em saúde utilizando ISO/IEC 27002

CEE78IS
Comissão de Estudo Especial
de Informática em Saúde

Sumário

1. Histórico do trabalho para adoção da norma ISO 27799:2008
2. Escopo da norma
3. Estrutura do documento

CEE78IS
Comissão de Estudo Especial de Informática em Saúde

1. Histórico do trabalho para adoção da norma ISO 27799:2008

- O primeiro projeto para adoção dessa norma, de nº 78:000.00-019, de Junho/2009, previsto para ser equivalente à ISO 27799:2008, foi encaminhado para Consulta Nacional, porém não passou no processo de revisão da ABNT e retornou para a CEE78 fazer uma análise mais rigorosa da tradução. Este trabalho foi paralisado em 2011.
- Na reunião do GT4, realizada em Julho/2014, foi apresentado o status do referido projeto e o grupo decidiu retomar esse trabalho.
- Essa norma foi, então, inserida no 1º lote de tradução pela empresa contratada. Sua versão em português foi analisada e discutida pelo especialista do GT4, Danilo Santos, e a empresa contratada até chegarem a versão final do texto-base ora apresentada.
- A versão final do texto-base foi então formatada pelos bolsistas do GT4 conforme regras estabelecidas pela ABNT.
- O segundo projeto para adoção no Brasil da norma ISO 27799 está sendo apresentado nesta Plenária da CEE78IS, no dia 15/09/2015.

CEE78IS
Comissão de Estudo Especial
de Informática em Saúde

2. Escopo da norma

- Especifica um conjunto detalhado de controles para a gestão da segurança de informação em saúde, e dá diretrizes de melhores práticas para segurança da informação em saúde, para organizações de saúde e curadores de informação pessoal de saúde, sobre como melhor proteger a confidencialidade, integridade e disponibilidade da informação de informação pessoal de saúde.
- A norma apresenta recomendações sobre como cada tópico deve ser tratado.
  - São discutidos tópicos como relacionamento com fornecedores, sistemas de criptografia, trabalho remoto, etc
- Se trata de uma norma simples e bem descritiva, de fácil leitura.

CEE78IS
Comissão de Estudo Especial
de Informática em Saúde

3. Estrutura do documento

Prefácio

Scope

General

Scope exclusions

Introdução

1 Escopo

1.1 Geral

1.2 Exclusões do escopo

2 Referências Normativas

3 Termos e definições

3.1 Termos de saúde

3.2 Termos de segurança da informação

CEE78IS
Comissão de Estudo Especial
de Informática em Saúde

3. Estrutura do documento

4 Termos abreviados

5 Segurança da informação em saúde

5.1 Metas da segurança da informação em saúde

5.2 Segurança da informação dentro da governança da informação

5.3 Governança da informação dentro da governança corporativa e clínica

5.4 Informação em saúde a ser protegida

5.5 Ameaças e vulnerabilidades na segurança da informação em saúde

6 Plano de ação prática para implementar a ISO/IEC 27002

6.1 Taxonomia das normas ISO/IEC 27002 e ISO/IEC 27001

6.2 Compromisso da direção na implantação da ISO/IEC 27002

6.3 Implantar, operar, manter e melhorar o ISMS

CEE78IS
Comissão de Estudo Especial
de Informática em Saúde

3. Estrutura do documento

6.4 Planejar: implantando o ISMS

6.5 Fazer: implantando e operando o ISMS

6.6 Verificar, monitorar e revisar o ISMS

6.7 Agir: mantendo e melhorando o ISMS

7 Implicações da ISO/IEC 27002 para a assistência médica

7.1 Geral

7.2 Política de segurança da informação

7.3 Organizando a segurança da informação

7.4 Gestão de ativos

7.5 Segurança em Recursos Humanos

7.6 Segurança física e ambiental

7.7 Gestão de comunicações e operações

CEE78IS
Comissão de Estudo Especial
de Informática em Saúde

3. Estrutura do documento

7.8 Controle de acesso

7.9 Aquisição, desenvolvimento e manutenção de sistemas de informação

7.10 Gerenciamento de incidentes de segurança da informação

7.11 Aspectos de segurança da informação para o gerenciamento da continuidade dos negócios

7.12 Conformidade

ANEXO A (informativo) - Ameaças à segurança da informação em saúde

ANEXO B (informativo) - Tarefas e documentos relativos da Gestão de Segurança de Sistemas de Informação

B.1 Tarefas e documentos relativos para a implantação do ISMS (Planejar)

B.2 Tarefas e documentos relativos para a implantação e operação do ISMS (Fazer)

CEE78IS
Comissão de Estudo Especial
de Informática em Saúde

3. Estrutura do documento

B.3 Tarefas e documentos relativos para a monitoração e revisão do ISMS (Verificar)

B.4 Tarefas e documentos relativos à manutenção e melhoria do ISMS (Agir)

ANEXO C (informativo) - Benefícios potenciais e atributos necessários das ferramentas de suporte

C.1 Benefícios potenciais das ferramentas de suporte

C.2 Atributos necessários das ferramentas de suporte

C.3 Suporte via ferramentas para processo ISO/IEC 27002

C.4 Suporte via ferramentas para o processo de análise de risco

Bibliografia

Normas relacionadas com a segurança da informação em saúde

Outras normas

CEE78IS
Comissão de Estudo Especial
de Informática em Saúde

Obrigado!

GT4 – Segurança da Informação e Paciente
gt4@cee78is.org.br