Padrões/normas de segurança

Existem padrões ou normas de segurança aceitos nacional ou internacionalmente?

Existem padrões de qualidade (ISO 9000 - para tudo) - (CMM/SPICE para software), etc. Existem normas equivalentes para segurança?

Existem duas normas ISO (famosas) que se referem a segurança de sistemas de informação:

- ISO 17799 - sobre os aspectos organizacionais e gerencias de segurança

- ISO 15408 - definições de componentes (técnicos) de segurança visando um processo de avaliação de sistemas. Também conhecido como Commom Criteria.

Outras normas :

- Generally Accepted System Security Principles ou GASSP (pre 99)

- Guidelines for the Management of IT Security , ou GMITS/ISO 13335

- BS7799-2 (mais sobre esse abaixo).

Por que padrões/normas?

Por que existem padrões e normas?

- para criar uma linguagem comum (todos nos sabemos o que é um metro, num projeto de engenharia pode-se esperar que todas as unidades estejam no SI (Sistema Internacional - mas veja algumas das explicações para a falha do Mars Polar Lander que caiu em Marte em 3/12/99).

- para poder-se comprar produtos que estão certificados num padrão (quando você compra um bujão de gás espera que ele siga as normas apropriadas de segurança, do tamanho da rosca, do conteúdo, etc)

- para poder certificar um produto que você vende (se você é o produtor do bujão acima, você precisa saber o que fazer para que seu bujão esteja certificado)

Estes objetivos também são válidos quando se fala em segurança de um sistema de informação

- deve haver um vocabulário comum para definir necessidades, características e violações de segurança.

- seria bom se fosse possível comprar sistemas de informações com certificados de segurança (isso basicamente não existe - mais abaixo).

- seria bom se existisse alguma norma que dissesse coisas como: o que é uma senha aceitável, quais algoritmos de criptografia são aceitáveis para transferir via Internet dados confidencias, quantos bits de resumo digital são necessários para garantir integridade de dados, etc. (isso não existe)

Existe uma consideração importante quando se fala de normalizações de segurança de sistemas de informação:

- é preciso fazer uma distinção importante entre sistemas de informação (programas) e o ambiente (computacional e organizacional) onde esses programas. Um programa pode ser segura mas rodar um ambiente que o torna inseguro - um programa exige senhas do seus usuários (e armazena as senhas de forma segura e confidencial) mas quando o programa foi instalado só se criou um usuário e uma só senha e todas as pessoas que tem que usar o programa se identificam para ele como sendo aquele único usuário e a senha é publicamente conhecida!

Portanto deve-se falar tanto numa certificação do software quanto numa certificação da empresa que vai usar o software.

Desta forma seria interessante que houvessem certificações tanto para produtos (comprar um produto certificado ou como certificar o produto que você vende), quanto para organizações (exigir que o seu parceiro de comércio eletrônico seja certificado ou como desenvolver a segurança interna para que sua empresa se certifique como segura - para sistemas de informação).

ISO17799 é uma norma para **organizações** mas não define o que seria uma certificação de segurança - portanto só cumpre o primeiro objetivo acima - cria uma linguagem comum para falar de segurança de organizações.

o ISO 15408 é uma norma para **produtos**. Veremos mais abaixo que ela define uma linguagem comum para falar principalmente de requisitos de segurança e como fazer avaliação de sistemas frente a estes requisitos.

Mas **nenhuma norma** vai em detalhes do tipo: quantos bits de resumo digital é necessário, ou de quanto em quanto a empresa deve pedir que seus funcionários troquem de senha, ou quantos backups devem ser mantidos, etc.

ISO 17799

Nome oficial: ISO/IEC 17799:2000

também é uma norma brasileira NBR ISO/IEC 17799(aproximadamente R$70,00 na ABNT).

Historia: A associação britânica de normas tinha 2 normas referentes a segurança de sistemas de informação a BS7799-1 e BS7799-2. A BS7799-1 foi submetida ao ISO como uma norma e aprovada com problemas para se transformar na ISO 17799. A BS7799-2 se referia especialmente ao processo de **certificação** do aspecto de segurança em **organizações** e não foi submetido para o ISO.

A ISO 17799 foi aprovada num processo chamado *fast track* onde não há tempo para se discutir e modificar a norma. Os EUA, Canadá e outros consideraram a norma incompleta e portanto inútil como norma.

O Brasil votou a favor da aprovação da norma.

A 17799 se refere a mecanismos organizacionais para garantir a segurança da informação. Não é uma norma que define aspectos técnicos de nenhuma forma, nem define as características de segurança de **sistemas**, apenas de **organizações**

A ISO 17799 esta dividida em 12 seções da seguinte forma:

1. Objetivo da norma

2. Termos e definições:

3. Política de segurança.

4. Segurança organizacional

5. Classificação e controle dos ativos de informação

6. Segurança de pessoas

7. Segurança física e do ambiente

8. Gerenciamento de operações e comunicações

9. Controle de acesso

10. Desenvolvimento de sistemas.

11. Gestão de continuidade de negócios:

12. Conformidade

Itens da ISO17799

Objetivo da norma: em particular contem a frase "tem como propósito prover uma base comum para o desenvolvimento de normas de segurança organizacional e da práticas efetivas de gestão da segurança"

Termos e definições: define os termos confidencialidade, integridade e disponibilidade

Política de segurança: indica que deve existir um documento sobre a política de segurança da empresa, e mecanismos de analise crítica das políticas implementadas

17799 - Segurança organizacional

Dividida nos seguintes ítens

- infraestrutura de segurança: indica que uma estrutura organizacional deve ser criada para iniciar e implementar as medidas de segurança. A norma lista algumas das tarefas desta coordenadoria de segurança, mas muitas de suas funções são também descritas em outros ítens.

- segurança no acesso de prestadores de serviço: garantir a segurança dos ativos acessados por prestadores de serviços.

- segurança envolvendo serviços tercerizados: deve-se incluir nos contratos de terceirização de serviços computacionais cláusulas para segurança.

17799 - Classificação e controle dos ativos de informação

- contabilização dos ativos: definir quais são os ativos de informação, seus responsáveis

- classificação dos ativos: assegurar que os ativos recebam um nível adequado de proteção

Um projeto de segurança tem que ter claro quais dados devem ser seguros, quão seguros, e quem é responsável pelos dados.

17799 - Segurança em pessoas

- segurança na definição e nos recursos de trabalho. Incluir preocupações de segurança quando contratar pessoas, isto inclui: incluir verificações de segurança na política de seleção, funcionários devem assinar acordos de confidencialidade, as definições de condições de trabalho deve incluir as responsabilidades de segurança dos funcionários.

- treinamento dos usuários: educação, conscientização e treinamento referentes a segurança

- respondendo a incidentes de segurança e mau funcionamento. É preciso que existam mecanismos para os usuários notificarem falhas

de segurança e mau funcionamento dos sistemas. É preciso que faça-se avaliações sobre essas notificações (mais sobre isso depois).

- finalmente convém que exista um processo disciplinar formal para funcionários que violaram a segurança.

Segurança física e de ambiente

- áreas de segurança: prevenir acesso não autorizado, dano e interferência nas instalações físicas. Isso inclui: definir um perímetro de segurança, controles de entrada física, etc

- segurança de equipamento: convém que equipamentos sejam fisicamente protegidos de ameaças e perigos ambientais. Isso inclui proteção roubo, fogo, e outros perigos ambientais, proteção tanto a falta de energia, segurança do cabeamento, definição de uma política de manutenção, proteção a equipamentos fora das instalações, e mecanismos para a alienação de equipamentos.

- controles gerais: coisas como deve-se usar proteção de tela com senha para evitar que informação não fique visível em tela, deve-se ter uma política quanto a deixar papeis na impressora por muito tempo, etc.

17799 - Gerenciamento das operações e comunicações

Esta é uma longa seção que descreve aspectos operacionais ligados a segurança.

- procedimentos e responsabilidades operacionais: definição dos procedimentos para a operação de sistemas. Isto inclui:
  - documentação dos procedimentos: os procedimentos devem estar documentados
  - controle de mudanças na documentação dos procedimentos

- procedimentos para o gerenciamento de incidentes: deve-se definir os procedimentos no caso de falha de sistema, não obtenção de serviço, erros resultantes de dados incompletos, e violação de confidencialidade. Os procedimentos devem conter planos de contingência para sanar o problema, a coleta de trilhas de auditoria, etc

- segregação funções: deve-se separar as pessoas que executam das pessoas que administram.

- separação de ambientes de operação e desenvolvimento: ferramentas de desenvolvimento não devem estar disponíveis nos ambientes de produção, etc

- planejamento e aceitação de sistemas: deve existir procedimentos formais para aceitar um sistema:

  - planejamento de capacidade: deve-se avaliar as necessidades computacionais, de telecomunicação do novo sistema, e verificar se elas são atendidas pela infraestrutura atual.

  - mecanismos formais para aceitar um novo sistema, atualizações e novas versões de um sistema já existente (mais sobre isso abaixo)

- proteção contra software malicioso: política e procedimentos para proteção contra vírus, incluindo proibição de uso e instalação de

software não autorizado, manutenção de anti-vírus, filtragem de e-mails, planos de contingência, etc.

- housekeeping (manutenção):

  - backups. manter um numero adequado de backups seja mantido em local remoto e protegido; verificar que as mídias de backup estão em bom estado; definir e executar periodicamente os procedimentos de recuperação de dados do backup.

  - registros de operação. atividade do pessoal de operação deve ser mantido

  - registros de falhas. todas as falhas devem ser notificadas. deve haver periodicamente uma analise critica destes registros

gerenciamento de redes.

gerenciamento e tratamento de mídias.

- gerenciamento de miúdas removíveis. mídias removíveis devem ser controladas fisicamente e armazenadas em local seguro

- descarte de mídia. deve haver procedimentos para o descarte seguro de mídias (papel, fitas, disquetes, CD, etc)

troca de informações e software

- contratos: toda troca de informação institucional entre empresas deve ser mediada pro um contrato que especifica as responsabilidades quanto a segurança de ambas as partes.

- segurança de mídias em transito: deve haver procedimentos para controlar que mídias em transito não sejam interceptadas, idas ou alteradas.

- segurança do comércio eletrônico: a norma lista uma serie de ítens que devem ser considerados quando se pensa em segurança de

comércio eletrônico. Curiosamente as considerações são colocadas como perguntas e não com afirmacões como no resto da norma.

- segurança de correio eletrônico: deve-se definir uma política de uso de correio eletrônico. Curiosamente, a norma sugere tanto que se use criptografia para proteger a integridade e confidencialidade das mensagens eletrônicas, e que se armazene as mensagens para serem usadas em caso de litígio.

17799 - Controle de acesso

- requisitos de negocio para controle de acesso: sem ser explicito a norma sugere que se use alguma forma de acesso baseado em papeis, desta forma num nível de política de acesso pode-se definir os direitos de cada papel.

- gerenciamento de acesso dos usuários

  – registro do usuário: ID única para cada usuário, pedir assinatura em termo de responsabilidade, remover usuário assim que o funcionário sair da empresa.

- gerenciamento de privilégios: aqui entras os papeis do controle de acesso baseado em papeis, mas basicamente se recomenda que usuários tenham apenas os privilégios necessários para fazer seu trabalho.

- gerenciamento de senhas: termo de responsabilidade deve afirmar que senha é secreta e não deve ser divulgada, senhas temporárias devem funcionar apenas uma vez.

- analise crítica dos direitos de acesso do usuário: deve-se analisar os direitos de acesso dos usuários com freqüência de 6 meses ou menos.

- responsabilidades dos usuários
  - senhas: a norma diz que é responsabilidade do usuário criar senhas boas (6 caracteres, não só letras, etc)
  - equipamento do usuário sem monitoração: o usuário deve ter cuidado com equipamento seu deixado sem monitoração (finaliza sessões ativas, colocar senha nos protetores de tela, etc)
- controle de acesso a rede. vários ítens sobre segurança de rede. Nós apenas listaremos os ítens, pois a norma não os discute em profundidade.

- política de utilização de serviços de rede
- rota de rede obrigatória
- autenticação para conexão externa de usuário
- autenticação de nó
- proteção de portas de diagnostico
- segregação de redes

  - controle de conexões de rede
  - controle de roteamento de rede
  - segurança de serviços de rede

- controle de acesso ao sistema operacional
  - identificação automática de terminal: nos casos onde deve-se conhecer onde um usuário se loga.

- procedimentos de entrada no sistema (log-on). sugestões como: limitar o numero de tentativas erradas para o log-on, não fornecer ajuda no processo de log-on, etc

- identificação de usuários: a não ser em casos excepcionais cada usuário deve ter apenas um ID. Considerar outras tecnologias de identificação e autenticação: smart cards, autenticação biometrica, etc

- sistema de gerenciamento de senhas: lista requisitos desejáveis para o componente que lê, armazena e verifica senhas, coisas como: não mostre a senha enquanto ela esta sendo digitada, armazene-as cifradas com um algoritmo unidirecional, etc

- uso de programas utilitários - programas utilitários são programas que se sobrepõem aos controles usuais (setuid root em unix, etc). tais programas devem ser removidos quando desnecessários, e só usados de forma limitada por usuários autorizados

- desconexão do terminal por inatividade. considerar tal limitação em áreas de alto risco

- limitação de tempo de conexão. considerar tal alternativa para aplicações sensíveis.

• controle de acesso às aplicações

- monitoração do uso e acesso ao sistema

  - registro de eventos (log): trilhas de auditoria registrando exceções e outros eventos de segurança devem ser mantidas por um tempo apropriado.

  - monitoração de uso do sistema: deve ser estabelecido procedimentos de monitoração de uso do sistema e o nível de monitoração deve ser mais intenso nas situações de maior risco. Uma analise critica dos log deve ser feita periodicamente. Convém que haja vários mecanismos de proteção à segurança do log.

  - sincronização de relógios: para garantir a corretude dos registros de auditoria

- computação móvel e trabalho remoto

  - usuários de equipamentos moveis (palmstops, laptops, etc) devem ser conscientização de praticas de segurança para tais equipamentos, incluindo criptografia, senhas, etc.

  - quando o funcionário trabalha remotamente, deve-se estender as preocupações e medidas de segurança intramuros sejam na medida do possível estendidas para o local remoto. Preocupações com métodos de acesso remoto seguro, manutenção de software e hardware, e copias de segurança são particularmente importantes.

17799 - Desenvolvimento e manutenção de sistemas

Este ítem lista algumas técnicas úteis para criar sistemas seguros. Deve-se comparar esta sessão com o ISO 15408 (Commom Criteria) a ser visto mais abaixo.

- requisitos de segurança de sistemas: aspectos de segurança devem ser considerados na fase de requisitos do sistema

- segurança nos sistemas de aplicação

  – validação de dados de entrada: programa deve valiadas dados lidos, aunto a valores, quantidade de dados etc.

- controle do processamento interno: os programas não devem assumir que dados permanecem inalterados e válidos entre chamadas do programa, ou mesmo durante a mesma execução do programa, e devem revalida-los.

- autenticação de mensagens: deve-se considerar uso de técnicas e autenticação de mensagens quando apropriado.

- validação de dados de saída.

• controles de criptografia

- política de uso de criptografia

  - criptografia

- segurança de arquivos de sistema

- segurança nos processos de desenvolvimento e suporte

17799 - Gestão da continuidade do negócio

Deve-se desenvolver planos de contingência para caso de falhas d segurança, desastres, perda de serviço, etc.

Estes planos devem ser documentados, e o pessoal relevante treinado. Os planos de contingência devem ser testados regularmente pois tais planos quando concebidos teoricamente podem apresentar falhas devido a pressupostos incorretos, omissões ou mudança de equipamento ou pessoal.

Os planos devem conter os seguintes ítens:

- condições para a ativação do plano

- procedimentos de emergência a serem tomados
- procedimentos de recuperação para transferir atividades essenciais para outras localidades, equipamentos, programas, etc.
- procedimentos de recuperação quando do estabelecimento das operações
- programação de manutenção que especifique quando e como o plano deverá ser testado
- desenvolvimento de atividades de treinamento e conscientização do pessoal envolvido

- designação de responsabilidades

17799 - Conformidade

- conformidade com requisitos legais: evitar violação de qualquer lei criminal ou civil, estatutos, regulamentação ou obrigações contratuais; evitar a violação de direitos autorais dos software - manter mecanismos de controle dos software legalmente adquiridos.

- analise crítica da política de segurança e da conformidade técnica

- considerações quanto à auditoria de sistemas

BS7799-2

O BS7799-2 é a segunda parte do padrão de segurança inglês cuja primeira parte virou o ISO 17799.

O BS7799 fala sobre certificação de segurança de organizações - isto é define quando e como se pode dizer que uma organização segue todo ou parte do ISO 17799 (na verdade do BS7799).

Nós não sabemos detalhes do processo de certificação, por exemplo se a certificação contempla conformidade parcial ou apenas total com a ISO 17799, etc. Segundo a British Standards (o BS), existem duas empresas certificadas no Brasil para dar certificados segundo o BS7799-2.

Há informações na Web que a British Standards **não** pretende submeter a BS7799-2 para a ISO.

ISO 15403 - Common Criteria

Historia: Vários países (EUA, Canadá, França, Inglaterra, Alemanha, etc) estavam desenvolvendo seus padrões para sistemas seguros (mas não militares). Nos EUA o padrão se chamada TCSEC (Trusted Computer System Evaluation Criteria), no Canadá CTCPEC, etc. Os países europeus decidiram unificar seus critérios, criando o Information Technology Security Evaluation Criteria (ITSEC). Mais tarde (1990) houve a unificação do padrão europeu e norte americano, criando- se assim o Common Criteria (CC). A versão 2.1 do CC se tornou o ISO 15408.

O 15408 é um conjunto de 3 volumes (aprox 400 paginas), onde o primeiro discute definições e metodologia, o segunda lista um conjunto grande de requisitos de segurança, e o terceiro fala sobre metodologias de avaliação.

Diferente do 17799, o CC é uma norma para definir e avaliar requisitos de segurança de sistemas, e não de organizações.

15408 - terminologia

O 15408 define uma serie de termos e abreviações que são necessárias para entender a norma.

- TOE - target of evaluation - é o sistema que esta sendo avaliado (ou definido)
- TSF - TOE security functions - é a parte de segurança do TOE - são estas funcionalidades que serão avaliadas
- ST - security target - é o conjunto de requisitos de segurança que o TOE deve satisfazer

- PP -protection profile - ST que estão pre-definidos (para aplicações genéricas como firewalls, etc).

15408 - especificação de requisitos

No CC, requisitos atômicos são chamados de componentes, e estão classificados em familias e, as familias em classes.

Como ilustração listaremos as 11 classes (com as 3 letras que as identificam), depois listaremos as familias de uma das classes (a FIA que é uma das de mais fácil compreensão e listaremos os componentes (os requisitos atômicos) de uma das familias.

- FAU - auditoria - requisitos sobre registros de eventos (log) e trilhas de auditoria. As familias desta classe se referem a escolha de eventos que serão registrados, analise de trilhas de auditoria, segurança dos logs, etc.

- FCS - suporte a criptografia - as duas familias falam sobre uso operacional de chaves criptográficas e gerenciamento das chaves

- FCO - comunicação - suporte a não repudiação e identidade das entidades envolvidas na comunicação.

- FDP - proteção de dados do usuário.

- FIA - identificação e autenticação - identificação de usuários

- FMT - gerenciamento de segurança - relativo a dados de segurança do TOE e o gerenciamento das outras classes

- FPR - privacidade - proteção quanto a descoberta por outros da identidade de um usuário.

- FPT - proteção das func,ões de segurança - proteção dos dados de segurança do TOE (em oposição aos dados do usuário - FDP)

- FRU - utilização de recursos - as familias desta classe falam sobre tolerância a falhas, prioridades e alocação de recursos

- FTA - acesso ao TOE - requerimentos de controle de acesso além dos definidos no FIA (identificação e autenticação).

- FTP - canais seguros - criação e uso de canais seguros (íntegros) de comunicação entre entidades do sistema - principalmente as TSF.

FIA

A classe FIA se preocupa com a identificação e autenticação de usuários (onde usuários não são necessariamente pessoas mas podem ser outros programas que fazem interface com o TOE).

A cada usuário estará associado um atributos de segurança (tipo identificação, grupo, papel, nível de segurança etc). O objetivo desta classe é: determinar e verificar a identidade de usuários, verificar sua autorização para interagir com o TOE, e atribuir o conjunto correto de atributos de segurança para cada usuário autorizado.

As familias são:

- FIA-UID - identificação do usuário - define em que condições o usuário precisa se identificar.

- FIA-UAU - autenticação do usuário - tipos de autenticação

- FIA-ATD - definição dos atributos do usuário - lista quais são os atributos de segurança

- FIA-SOS - especificação de segredos

- FIA-USB - ligação entre usuário e sujeito

- FIA-AFL - falhas de autenticação - numero máximo ou tempo máximo para tentativas de autenticação e o que fazer

FIA-UAU

Define os tipos de autenticação.

- FIA-UAU.1 - tempo da autenticação - permite o usuário a fazer certas ações antes da autenticação
- FIA-UAU.2 - autenticação antes de ações
- FIA-UAU.3 - proteção contra autenticação forjada - o sistema deve identificar e impedir o uso de dado de autenticação que foi forjado ou copiado

- FIA-UAU.4 - autenticação de um uso apenas - autenticação opera com dados que só podem ser usados uma vez (one-time passwords)

- FIA-UAU.5 múltiplas autenticações - mais de uma forma de autenticação é necessária para alguns eventos

- FIA-UAU.6 - re-autenticação - é possível pedir que o usuário se autentique de novo antes de eventos definidos

- FIA-UAU.7 - proteção quanto a feedback - pouca informação é fornecida ao usuário durante o processo de autenticação

CC -especificação - resumo

Resumindo uma especificação de funcionalidades de segurança (ou um ST em CC) é um conjunto de componentes tais como FAI-UAU.5, FIA-USB.x,FDP-XXX.x, etc, etc.

ST já predefinidos por grupos internacionais, para aplicações gerais, são chamados PP (protection profiles). Existe mecanismos para definir e submeter novos PP. Existem PP para

- bancos de dados relacionais
- firewalls

- smart cards
- sistemas de controle de acesso baseado em papeis
- etc.

CC - avaliação

A terceira parte do ISO 15408 trata de avaliação de sistemas (ou TOEs). Nós não entraremos em detalhes da parte de avaliação, mas ela contem classes similares as de especificação, mas as classes de avaliação se referem a coisas como: gerenciamento de configuração, entrega e instalação do software, desenvolvimento, documentação, etc.

Mais importante é que a norma define diferentes níveis de confiança (assurance) na avaliação.

Os níveis são os seguintes:

- EAL1 - testado funcionalmente - as funcionalidades de segurança são testadas no produto pronto e sem acesso maior ao desenvolvedor ou ao código fonte

- EAL2 - testado funcionalmente e estruturalmente - o desenvolvedor fornece dados a respeito da estrutura do programa e dados de testes dos componentes

- EAL3 - testado e verificado metodicamente - o desenvolvedor deve mostrar mais sobre o processo de desenvolvimento, gerenciamento de configuração, e alguns dos resultados de testes do desenvolvedor devem ser verificados independentemente

- EAL4 - desenhado, testado e revisto metodicamente - detalhes da estrutura do programa são todos disponíveis, testes são verificados independentemente, desenvolvedor deve mostrar o uso de boas praticas de segurança no desenvolvimento do sistema

- EAL5 - desenhado e testado semi-formalmente - deve-se mostrar a correspondência entre os requisitos de segurança e os componentes do programa.

- EAL6 - desenho e testado de forma verificada e semi-formal

- EAL7 - desenho e testes formalmente verificados

Na pratica, avaliações são feitas no nível EAL2 (por exemplo a avaliação feita pela Computer Science Corporation do firewall da Lucent)

EAL3 parece ser o máximo possível para sistemas legados.