

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

**1.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”

**2.Termos e definições:** define os termos confidencialidade, integridade e disponibilidade

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

## 4. Segurança organizacional

Dividida nos seguintes itens

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

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

## 5. 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.

## 6. 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.

## 7. 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.

## 8. 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 mídias 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 por um contrato que especifica as responsabilidades quanto a segurança de ambas as partes.
  - segurança de mídias em trânsito: deve haver procedimentos para controlar que mídias em trânsito não sejam interceptadas, lidas ou alteradas.

- segurança do comércio eletrônico: lista uma serie de itens que devem ser considerados quando se pensa em segurança de comércio eletrônico. Curiosamente as considerações são colocadas como perguntas e não com afirmações 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.

## 9. 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 entram os papéis do controle de acesso baseado em papéis, mas basicamente recomenda-se que usuários tenham apenas os privilégios necessários para fazer seu trabalho *least privilege*
  - gerenciamento de senhas: termo de responsabilidade deve afirmar que senha é secreta e não deve ser divulgada, senhas temporárias devem funcionar apenas uma vez.
  - análise crítica dos direitos de acesso do usuário: deve-se analisar os direitos de acesso dos usuários com frequência 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 (finalizar sessões ativas, colocar senha nos protetores de tela, etc)
- controle de acesso a rede. vários itens sobre segurança de rede. Nós apenas listaremos os itens, 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 diagnóstico
- 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 biométrica, 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 análise crítica 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 conscientizados 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.

## 10. Desenvolvimento e manutenção de sistemas

Este item lista algumas técnicas úteis para criar sistemas seguros. Deve-se comparar esta sessão com o ISO 15408 (Common Criteria)

- 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 validar dados lidos, quanto 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 revalidá-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

## 11. Gestão da continuidade do negócio

Deve-se desenvolver planos de contingência para caso de falhas de 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 itens:

- 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

## 12. 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.
- análise crítica da política de segurança e da conformidade técnica
- considerações quanto à auditoria de sistemas

## ISO 2700X

ISO 27001 - BS 7799-2 (certificação de segurança)

ISO 27002 - ISO 17799 (2005) (boas práticas)