2.0 - Organizações e Padrões de Segurança da Informação

prof. Fábio Engel

fabioe@utfpr.edu.br

Conteúdo

Organizações e Padrões de Segurança da Informação

Organizações e Padrões de Segurança da Informação

- Organizações atuais obtém partes de sua infraestrutura de TI de vários fornecedores - e esperam que esses produtos funcionem juntos. Isto é possível devido aos diversos padrões eu garantem a compatibilidade entre produtos de diferentes países e fornecem diretrizes para garantir que produtos e ambientes computacionais atuais funcionem juntos.
- A seguir, veremos alguns padrões comuns para produtos e serviços de computador e de rede, especificamente sobre aqueles que se relacionam com a segurança.

NIST

- NIST (*National Institute of Standards and Technology* - Instituto Nacional de Padronização e Tecnologia)
  - Órgão federal do departamento de comércio dos EUA.
  - Fornece padrões para medição e tecnologia sobre os quais recaem quase todos os dispositivos de computação.
  - Em 1990 estabeleceu uma coleção de documentos chamada de Publicações Especiais série 800, para fornecer uma identidade separada para publicações de segurança de tecnologia de informação. A tabelas a seguir exibem alguns dos recursos encontrados nessa série.

NIST

Número	Título
800-61 Rev.1	Guia para tratamento de incidentes em segurança computacional.
800-78-2	Algoritmos criptográficos e tamanhos de chave de verificação de identidade pessoal (PIV).
800-115	Guia técnico para teste e avaliação de segurança de informação.
800-121	Guia para segurança de bluetooth.
800-122	Guia para proteção da confidencialidade de informações pessoalmente identificáveis (PII).

IEC

- IEC (*International Electrotechnical Commission* - Comissão Eletrotécnica Internacional)
  - Organização predominante para desenvolver e publicar padrões internacionais para tecnologias relacionadas com dispositivos e processos elétricos e eletrônicos.
  - Trata de uma ampla diversidade de áreas, incluindo: Geração de energia; Transmissão e distribuição de energia; aparelhos elétricos comerciais e de consumidores; Semicondutores; Baterias; Energia Solar; Telecomunicações;
  - Você provavelmente encontrará padrões IEC relativos a hardware de computador e de redes.
  - https://www.iec.ch/cyber-security

W3C

- W3C (*World Wide Web Consortium* - Consórcio da World Wide Web)
  - Fundado em 1994 por Sir Tim Berners-Lee.
  - Principal organização internacional de padrões para a World Wide Web.
  - Tem como finalidade desenvolver protocolos e diretrizes que unifiquem a World Wide Web e garantam seu crescimento a longo prazo.
  - Entre seus padrões estão: CSS, HTML e XML.
  - https://www.w3.org/Security/

IETF

- IETF (*Internet Engineering Task Force* - Força-Tarefa de Engenharia da Internet)
  - Desenvolve e promove padrões para a Internet.
  - A IETF se reuniu inicialmente em 1986, como um grupo de 21 pesquisadores que desejavam formalizar os principais protocolos de comunicação da Internet. Hoje, há vários grupos de trabalho (*Working Group* - WG), e cada um trata de um assunto específico.
  - Cada WG tem uma lista de correspondência dedicada, na qual qualquer pessoa pode se inscrever. Essas listas servem como meio de comunicação principal para os participantes.
  - https://www.ietf.org/topics/security/

IETF

- A IETF produz Solicitação por Comentários (RFC - *Request for comments*).
- Uma RFC é uma série de documentos que variam desde memorandos simples até documentos de padrões.
- A IETF publica orientações para RFCs. Aqui estão alguns pontos sobre RFCs:
  - Apenas algumas RFCs são padrões - Apenas as que iniciam com frases do tipo "Este documento especifica..." ou "Este memorando documenta..." devem ser considerados padrões ou documentos normativos.
  - RFCs nunca mudam - Qualquer mudança em uma RFC recebe um novo número e se torna uma nova RFC.
  - RFCs podem ter origem em outras organizações - A IETF cria apenas algumas RFCs.

IETF

- RFCs que definem padrões formais possuem quatro estágios:
  - Padrão Proposto (PS - *Proposed Standard*) - O Estágio inicial oficial de um padrão.
  - Padrão em Rascunho (DS - *Draft Standard*) - O segundo estágio de um padrão, após os participantes terem demonstrado que o padrão foi implantado em ambientes de trabalho.
  - Padrão (STD - *Standard*) - O estágio final de um padrão, após ele ter se mostrado amplamente adotado e implantado.
  - Melhor Prática Atual (BCP - *Best Current Practice*) - O método alternativo usado para documentar especificações operacionais que não sejam padrões formais.
  - https://www.rfc-editor.org/

IAB

- IAB - (*Internet Architecture Board* - Grupo de Arquitetura da Internet)
  - Subcomitê da IETF e também serve como órgão consultivo para a Sociedade da Internet (ISOC - *Internet Society*).
  - O IAB serve como comitê supervisor para muitas atividades da IETF e fornece supervisão para:
    - Arquitetura para protocolos e procedimentos da Internet
    - Processos usados para criar padrões
    - Procedimentos editoriais e de publicação para RFCs
    - Confirmação do presidente e de diretores técnicos de áreas da IETF.

IEEE

- IEEE - (*Institute of Electrical and Electronics Engineers* - Instituto de Engenheiros Eletricistas e Eletrônicos)
  - Maior associação profissional do mundo para o avanço de tecnologia.
  - O IEEE apóia 38 sociedades que focalizam atividades em áreas técnicas específicas, que incluem magnética, fotônica e computação. Cada sociedade desenvolve publicações, realiza conferências e promove atividades e eventos para promover o conhecimento e o interesse em uma área específica.
  - Também é umas das maiores organizações de produção de padrões, como por exemplo o IEEE 802 LAN/MAN

ITU-T

- ITU (*International Telecommunication Union* - União Internacional de Telecomunicações)
  - Órgão das Nações Unidas responsável por administrar e promover questões de informação e tecnologia.
  - A atividade mais antiga e reconhecida da ITU é seu trabalho no desenvolvimento de padrões.
  - O Setor de Telecomunicações da ITU (ITU-T - ITU Telecomunnication Sector) realiza todo o trabalho de padrões da ITU.

ITU-T

- O ITU-T divide suas recomendações em 26 séries separadas, cada uma com uma letra exclusiva do alfabeto. Por exemplo, recomendações de comutação e sinalização estão na série Q. Recomendações de redes de dados, comunicações de sistemas abertos e de segurança estão na série X.
- Três recomendações de interesse em segurança da informação são:

Recomendação da ITU-T	**Descrição**
X.25	Descreve conjunto de protocolos para comunicação de uma rede remota de comutação de pacotes.
X.75	Descreve o protocolo para conectar duas redes X.25
X.509	Recomendação para uma infraestrutura de chave pública (PKI)

ANSI

- ANSI (*American National Standards Institute* - Instituto Nacional Americano de Padronização)
  - Seu objetivo é fortalecer o mercado americano na economia global. Ao mesmo tempo, se empenha para garantir a segurança e a saúde de consumidores e a proteção do ambiente, promovendo padrões de consenso voluntário e sistemas de avaliação de conformidade.
  - Padrões ANSI importantes:

Padrão	**Descrição**
Código ANSI	Padrão que define um conjunto de valores usados para representar caracteres em computadores
Padrão Americano de FORTRAN	O padrão americanos de FORTRAN foi a primeira linguagem de programação-padrão
C ANSI	ANSI publicou C ANSI como uma versão-padrão da linguagem de programação C em 1989

Padrões de segurança

ISO 17799

- **ISO 17799** é um padrão internacional de segurança que documenta um conjunto abrangente de controles que representam melhor práticas em sistemas de informação. O padrão, na realidade, consiste em duas partes separadas:
  - O código de prática ISO 17799.
  - A especificação BS 17799-2 para um sistema de gerenciamento de segurança de informação.
- A finalidade principal do padrão é identificar controles de segurança necessários para sistemas de informação em ambientes atuais de negócios.
- A ISO 17799 deu a muitas organizações uma estrutura sobre a qual construir sua política de segurança.
- O padrão permitiu que clientes em potencial avaliassem organizações em seus respectivos esforços em direção à proteção de dados.

ISO 17799

- A ISO divide o padrão em 10 seções principais
    1- **Política de Segurança** - Declaração de orientação de gerenciamento.
    2- **Organização de Segurança** - Governança de segurança de informação ou como segurança de informação deve ser imposta.
    3- **Classificação e controle de ativos** - Procedimentos para classificar e gerenciar ativos de informação.
    4- **Segurança de Pessoal** - Diretrizes para controles de segurança que protegem e limitam pessoas.
    5- **Segurança física e ambiental** - Proteção de instalações de computação.

ISO 17799

- A ISO divide o padrão em 10 seções principais
  6- **Gerenciamento de comunicações e operações** - Gerenciamento de controles de segurança técnicos em sistemas e redes.
  7- **Controle de acesso** - Controles que limitam direitos de acesso a recursos de rede, aplicativos, funções e dados.
  8- **Desenvolvimento e manutenção de sistema** - Diretrizes para projeto e incorporação de segurança em aplicativos.
  9- **Gerenciamento de continuidade de negócios** - Proteção, manutenção e recuperação de processos e sistemas críticos para empresas.
  10- **Conformidade** - Garantia de conformidade com políticas, padrões, leis e regulamentações de segurança de informação.

ISO 17799

- Um padrão mais recente, a **ISO/IEC 27002**, substituiu a ISO 17799 e fornece um padrão de segurança da informação genérico, acessível por toda organização, independente de tamanho, setor ou localização.
- Embora a ISO/IEC 27002 tenha substituído a ISO 17799, você ainda verá referências a ISO 17799 como importante padrão em segurança da informação.

- **ISO/IEC 27002**
  - A série ISO/IEC 2700 é uma família crescente de padrões gerais de segurança de informação.
  - ISO/IEC 27002 é o "Código de Prática de Técnicas de Segurança de Tecnologia de Informação para Gerenciamento de Segurança de Informação".
  - ISO/IEC 27002 fornece a organizações recomendações de melhores práticas sobre gerenciamento de segurança da informação. O padrão direciona suas recomendações para pessoal responsável por sistemas de gerenciamento de segurança de informação.

ISO/IEC 27002

- ISO/IEC 27002 expande o âmbito de seu predecessor, acrescentando duas novas seções e reorganizando várias outras. A ISO divide o novo padrão em 12 seções principais:
    1- **Avaliação de risco** - Métodos formais de identificação e classificação de risco.
    2- **Política de segurança** - Declaração de orientação gerencial.
    3- **Organização de segurança da informação** - Governança de segurança de informação ou como a segurança de informação deve ser imposta.
    4- **Gerenciamento de ativos** - Procedimentos para adquirir, classificar e gerenciar ativos de informação.

- [continuação...]
  5- **Segurança de recursos humanos** - Diretrizes de segurança para pessoal que entra, sai ou muda de função em uma organização.
  6- **Segurança física e ambiental** - Proteção de instalações computacionais.
  7- **Gerenciamento de comunicações e operações** - Gerenciamento de controles de segurança técnicos em sistemas e redes.
  8- **Controle de acesso** - Controles que limitam direitos de acesso a recursos de rede, aplicativos, funções e dados.

ISO/IEC 27002

- [continuação...]
  9- **Desenvolvimento e manutenção de aquisição de sistemas de informação** - Diretrizes para projeto e incorporação de segurança em aplicativos.
  10- **Gerenciamento de incidentes de segurança de informação** - Antecipação e resposta adequadas a brechas de segurança de informação.
  11- **Gerenciamento de continuidade de negócios** - Proteção, manutenção e recuperação de processos e sistemas críticos para empresas.
  12- **Conformidade** - Garantia de conformidade com políticas, padrões, leis e regulamentações.

Resumo

- **Resumo do conteúdo**
  - Diversas organizações definem padrões que documentam especificações técnicas ou outros critérios específicos para uso, como regras, diretrizes ou definições de características. Organizações e indústrias também usam padrões para garantir que produtos e serviços sejam consistentes. A capacidade de diferentes produtos de diferentes organizações funcionarem junto depende de padrões. À medida que a indústria de TI avança, também aumenta a necessidade de padrões novos e atualizados.

Referências

- Fundamentos de Segurança de Sistemas de Informação - David Kim; Michael G. Solomon