FLUIDEZ NAS COMUNICAÇÕES

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

Utilização da Normalização na Regulação das Comunicações Eletrónicas

Segurança e Integridade de Redes e Serviços

Workshop ANACOM – *it*SMF Portugal:

Normalização de TI – técnicas de segurança

Manuel Pedrosa de Barros
Direcção de Segurança nas Comunicações

Normalização – artigo 29.º

ANACOM

A ARN deve:

- Incentivar utilização de **normas técnicas** não imperativas e especificações

Para:

- Assegurar a interoperabilidade dos serviços
- Aumentar a liberdade de escolha dos utilizadores

A fim de:

- Encorajar a oferta harmonizada de redes e serviços de comunicações eletrónicas e recursos e serviços conexos

Normalização – fontes

ANACOM

Organizações europeias de normalização:

- CEN
- CENELEC
- ETSI

Em falta destas:

- UIT
- CEPT
- ISO
- IEC

Sem prejuízo, podem ser emitidas especificações técnicas a nível nacional

Segurança e Integridade

ANACOM

Operadores e Prestadores de Serviço:

- Adopção de **MEDIDAS TÉCNICAS E ORGANIZACIONAIS**

  (baseadas)

  - Análise e gestão do risco
  - Estado da técnica (evolutiva)

  (objectivo)

  - Impedir/minimizar **impacto incidentes de segurança**
    - nos **utilizadores** e
    - nas **redes interligadas**

Segurança e Integridade

ANACOM

Operadores:

- Adopção de **MEDIDAS DE GARANTIA DE INTEGRIDADE DAS REDES**
- (objectivo)
  - Assegurar a **continuidade do fornecimento dos serviços** que utilizam essas redes

HARMONIZAÇÃO E NORMALIZAÇÃO

- **MEDIDAS DE EXECUÇÃO** aprovadas pela Comissão Europeia mediante parecer da ENISA
  - No caso das Notificações:
    - Circunstâncias, formato, procedimentos aplicáveis
- **Normas técnicas**
  - Europeias (CEN, CENELEC, ETSI, …) ou
  - Internacionais (ISO/IEC, UIT, IETF, …)

Segurança e Integridade

ANACOM

A Autoridade Reguladora pode determinar:

- Elaboração de **plano** atualizado que contemple as medidas adotadas
- Realização de **exercícios** de avaliação e melhoria das medidas adotadas
- Realização **auditoria à segurança** redes e serviços
  - Req.: âmbito, periodicidade, procedimentos e normas de referência, entidades auditoras

Segurança e Integridade

ANACOM

- *"Technical Guideline for Minimum Security Measures"*, ENISA
- Domínios:
  - Governança e gestão de risco
  - Segurança dos recursos humanos
  - Segurança de sistemas e instalações
  - Gestão de operações
  - Gestão de incidentes
  - Gestão da continuidade do negócio
  - Monitorização, auditoria e teste

Referências: normas

ANACOM

- **ISO/IEC 27000:2012** – IT - Security techniques -- Information security management systems – Overview and vocabulary
- **ISO/IEC 27001/2:2005** – IT - Security techniques -- Information security management systems – Requirements / Code of practice for information security management
- **ISO/IEC 27005:2011** – IT - Security techniques - Information security risk management
- **ITU-T Rec. X.1055 (11/2008)**: Risk management and risk profile guidelines for telecommunication organizations
- **ISO/IEC 24762:2008** - IT — Security techniques — Guidelines for information and communications technology disaster recovery services
- **ISO/IEC 27031:2011** - IT -- Security techniques -- Guidelines for information and communication technology readiness for business continuity

Referências: normas

ANACOM

- **ISO/IEC 27031:2011** - IT -- Security techniques -- Guidelines for information and communication technology readiness for business continuity
- **ITU-T Rec. X.1056 (01/2009)** - Security incident management guidelines for telecommunications organizations
- **ITU-T Rec. X.1051 (02/2008)**, Telecommunication security – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- **BS 25999 – 1/2** - Business Continuity Management
- **NICC ND 1643** - Minimum security standards for interconnecting communications providers
- **CobiT –** Control Objectives for Information and related Technology - ISACA

FLUIDEZ NAS COMUNICAÇÕES

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

Obrigado !

Workshop ANACOM – *it*SMF Portugal:

Normalização de TI – técnicas de segurança

Manuel Pedrosa de Barros
Direcção de Segurança nas Comunicações