IT Security at 360 degrees

Course Program

1. Introduction to information security
   a) Technical and management security
   b) Politics, roles, responsibility and risks
   c) Security and trust
   d) threats, vulnerabilities and countermeasures
2. Viruses
   a) Programs
   b) GUI
   c) File types
   d) viruses and penetration techniques
   e) principal defences for personal computer user
   f) Types of attack code: virus, worm etc.
   g) anti-virus
3. Cryptography
   a) confidentiality, authenticity, integrity
   b) principles and ingredients
   c) Caesar and One-Time-Pad cipher
   d) Kerchoff's principle
   e) types of algorithms
   f) symmetrical algorithms
   g) a-symmetrical algorithms (RSA)
   h) hash algorithms
   i) MAC e H-MAC
   j) use of the cryptographic algorithms
4. Authentication and access control
   a) identification, authentication, authorization

b) password, keys, biometry

c) network authentication

5. Public key infrastructures (PKI)

a) Certification Authority and Registration Authority

b) LDAP e X.500

c) Web of trust

6. Network security

a) Firewall and perimeter defence

b) firewall architectures

c) Proxy and Application Layer Gateway

d) Intrusion Detection System andIntrusion Prevention System

e) local and wide area networks

f) wireless

g) principal network attacks

7. Data and resources disponibility

a) disponibility and resilience

b) business continuity and disaster recovery

c) hardware infrastructures and system management

d) duplication, backup and data preservation