NATIONAL UNIVERSITY OF ENGINEERING
COLLEGE OF INDUSTRIAL AND SYSTEMS ENGINEERING
SYSTEMS ENGINEERING PROGRAM

ST215 – INFORMATION SECURITY

I. GENERAL INFORMATION

CODE	:	ST215 Information Security
SEMESTER	:	9
CREDITS	:	3
HOURS PER WEEK	:	4 (Theory–Practice)
PREREQUISITES	:	ST334 Data Communication Systems
CONDITION	:	Compulsory
DEPARTMENT	:	Systems and Telematics

II. COURSE DESCRIPTION

The course prepares students for understanding and applying the concepts, tools and methods for the analysis and design of information security systems based on the identification and assessment of the potential threats and risks affecting the information system, and considering its life-cycle in the development of the system. National and international norms and standards are used including NTP 17799, ISO/IEC 27001, as well as recommended “good practices” for the management of information security. Students work in teams for completing and defending the design of an information security system.

III. COURSE OUTCOMES

At the end of the course, students:

1. Understand and apply the concepts of information security.
2. Analyze the background, scope and components of an information security problem.
3. Identify the information assets subject to security risks and threats.
4. Identify the threats and vulnerabilities that could affect the confidentiality, integrity and availability of information systems.
5. Identify and propose information security policies to be used for the logic design of the solution.
6. Propose contingency strategies, incident responses, disaster recovery responses for ensuring business continuity.
7. Assess and evaluate information security technologies that better fit to the particular organization or enterprise.
8. Develop and implement information security solutions applying project management method for ensuring of the project.

IV. LEARNING UNITS

1. INTRODUCTION TO INFORMATION SECURITY

History of information security / Concepts and key issues in information security / Security in the life-cycle in software development / Role of information security professionals / Entrance test / Video.

2. NEED FOR INFORMATION SECURITY

Security and quality / Quality tools for problem solving / Seven-steps method for quality improvement / First point is business needs, after it is technology needs / Threats and Risks / Categories of information security threats / Attacks / Attack sources and description.

3. **LEGAL, ETHICAL AND PROFESSIONAL ISSUES**
   Definitions: law, ethics / Types of law / Applicable laws / Privacy / Information freedom / Personal data protection law / International laws / Intellectual property rights / Digital Property rights / Sarbanes-Oxley Act / Peruvian regulations / Peruvian Bank and Insurance Surveillance / United Nations Chart / Politics vs Law / Ethics and professional ethics / Ethic codes / Professional certification and organizations.

4. **RISK MANAGEMENT I**
   Risk management / Knowing us and knowing the enemy / Responsibilities and duties of risk management / Risk management process / Threats identification / Assets identification and valuation.

5. **RISK MANAGEMENT II**
   Risk control strategies: avoid or evade, transfer, mitigate / Incident response plan IRP / Disaster recovery plan DRP / Business continuity plan BCP / Mitigation strategies / Decision milestones for risk management / Risk control cycles / Control categories / Control functions: preventive, detective, corrective / Risk control layers / Dimensions of information security / Feasibilities studies / Cost-Benefit analysis / Benchmarking / Base line / Technical feasibility.

6. **SECURITY POLICIES**
   Policies, standards, guides and procedures / Specific problem policy / Specific system policy / Access control policy / Policy management / Information classification / System design / Information security models / ISO 17799, NIST, VISA, IETF / Use and protection environment / Controls / Security training / Developing security awareness / Security architecture.

7. **DISASTER RECOVERY AND BUSINESS CONTINUITY**
   Contingency plan / Action workteams / Incident response plan IRP / Disaster recovery plan DRP / Business continuity plan BCP / Analysis of business impact / Identification of threats and attacks / Analysis of business units / Attack scenarios / Potential damage assessment / Classification of response plans / Incident detection / Continuity strategies / Models IR, DR, BC.

8. **PHYSICAL DESIGN: SECURITY TECHNOLOGIES**
   Firewalls / First generation: Packet filtering / Second generation: Proxy applications / Third generation: Total inspections / Fourth generation: Dynamic filtering / Fifth generation: Kernel proxy (protocols pile) / Packet filtering router / Intruder detectors / Analysis and scanning tools / Encryption / Algorithms / Standards / Public key infrastructure / IP security / Biometrics.

9. **PHYSICAL DESIGN: PHYSICAL SECURITY**
   Community roles / Access control / Facilities management / Identification cards and tokens / Closing and keys / Intruders traps / Monitoring and surveillance / Alarms / Walls / Fire prevention, detection and suppression / Air conditioning / UPS / Remote computing Energy management.

10. **SECURITY IMPLEMENTATION**
    Project management / Security plan development and deployment / Financial and budget issues / Schedules / Personnel / Logistics / Organizational feasibility / Training / Change and technology control / Supervision / Feedback cycle / Bull eye model / Change resistance.

11. **SECURITY AND PERSONNEL**
    Information security within organizations / Problems and worries regarding personnel competencies and selection / Specialization and certifications

V. LABORATORY AND PRACTICAL EXPERIENCES

Laboratory: Use of project management software applications.
Student project: Design of a security information system for an enterprise. Work team up to four students.

VI. METHODOLOGY

The course is carried out in theory and practice sessions. In theory sessions, the instructor presents the concepts, methods and techniques. In practice sessions, instructors and students analyze and solve diverse problems and issues related to information security. Students work in teams to develop and complete the design of the information security system for a given company whose core business is information and communication technologies. At the end of the course, each student team must submit and defend the design project. In all sessions, students' active participation is encouraged and graded.

VII. EVALUATION FORMULA

The Final Grade PF is calculated as follows (evaluation system: F):

$$\boldsymbol{PF} = (\boldsymbol{PP} + \boldsymbol{EP} + \mathbf{2}\ \boldsymbol{EF})/\mathbf{4}$$

EP: Mid-term exam EF: Final exam
PP: Average of quizzes and final report

VIII. BIBLIOGRAPHY

1. **D. GOLLMANN**
   Computer Security.
   John Willey & Sons 2011.
2. **C.P. PEEGER et. al.**
   Security in Computing
   Prentice Hall Editions 2006
3. **WHITMAN, MICHAEL E. & MATTORD Herbert**
   Principles of Information Security
   Thompson Course Technology, Boston, MA, 2011