- Introduzione alla Continuità Operativa: Alta Affidabilità, Fault Tolerance, Business Continuity e Disaster Recovery
- La Gestione del Rischio:
  - Scope, Asset e Classificazione dell'Informazione
  - Risk Assessment, Gap Analysis, Risk Treatment e Reduction
  - Esempi di Calcolo del Rischio: con metodi artigianali e mediante strumenti SW commerciali
  - L'Analisi del Rischio secondo gli standard ISO 31000 e ISO/IEC 27005
- L'organizzazione delle attività di Vulnerability Assessment e Penetration Test
- La definizione di un modello di Information Security Governance:
  - Contromisure ispirate alla Defense in Depth e Maturity Model
  - Requisiti e Policy per la Sicurezza delle Informazioni
  - Strumenti SW a supporto delle conformità di legge
  - Vulnerability Management & Exposure, Virtual Patching
- Etica nell'Informatica: i pericoli della Tecnomediazione, il Codice Etico, i nuovi interrogativi posti dai sistemi autonomi e robotizzati

Principali competenze apprese:

- Conoscere approfonditamente la natura di un ISMS coerente con le norme e le best practice internazionali e saperlo implementare e gestire in un'organizzazione

---

II.6 Business Continuity and Crisis Management

Responsabile: Susanna Buson
Ore: 16
(12 ore D.ssa Susanna Buson, 4 ore Dr. Diego Marson)

Pre-requisiti:

- Nessuno

Programma:

- Concetti di Business Continuity
- Standard 22301
- Metodologia per la gestione di Programma di Business Continuity (basato sulle GPG 2018 del Business Continuity Institute)
- Policy di Business Continuity
- Ruoli e responsabilità nella Business Continuity
- Business Impact Analysis e Risk Assessment
- Progettazione di soluzioni di continuità
- Realizzazione di soluzioni di continuità
- Esercitazione e test
- Miglioramento continuo
- L'incorporazione della Business Continuity nella cultura aziendale

- Concetti di Crisis Management
- Esercitazione Table Top di Crisis Management
- Definizione di SOC e CERT e interazione con la Business Continuity attraverso il processo di gestione degli incidenti e di escalation

Principali competenze apprese:

- Competenza base per il professionista della Business Continuity

---

II.7 Legal Informatics, Privacy and Cyber Crime

Responsabile: Elena Bassoli

Ore: 36

- **(8 ore Avv. Elena Bassoli, 4 ore Ing. Ermete Meda, 4 ore Ing. Roberto Surlinelli, 8 ore Prof. Rodolfo Zunino, 8 ore Studio Legale Losengo Soliani, Avv. Elisa Marini, Avv. Vincenzo Morgione, 4 ore Dr. Giorgio Volta)**

Pre-requisiti:

- Nessuno

Programma:

- (Losengo) Le basi del diritto penale: reati, delitti e contravvenzioni, depenalizzazione 2016, elementi soggettivi ed oggetti di reato. Concetto di imputabilità. Tipologia di sanzioni.
- (Losengo) Reati ordinari in Rete: diffamazione, ingiuria, sostituzione di persona, atti persecutori.
- (Losengo) I crimini informatici: L. 547/1993.
- (Surlinelli) La Convenzione di Budapest e la L. 48/2008: metodologie di acquisizione delle prove digitali
- (Surlinelli) La pedopornografia: L. 38/2006.
- (Zunino) Caratteristiche del Cybercrime, e genesi del Cybercrime e Identità Digitale,
- (Bassoli) La tutela del software e delle opere dell'ingegno ex L. 633/1941.
- (Bassoli) La tutela dei dati personali nel nuovo Regolamento europeo 2016/679 (GDPR) e decreto legislativo di adeguamento n. 101/2018.
- (Bassoli) Convenzione internazionale di Budapest del 2001 contro il Cybercrime. L. 48/2008 di sottoscrizione, Dir. UE 2016/680 sui dati personali e le forze di polizia
- (Meda) La norma internazionale IEC 62443 sulla Cybersecurity Industrial e panoramica sulla legislazione internazionale ed europea in materia di Cybersecurity: direttive NIS e NIST, GDPR, Cybersecurity Act e Cybersecurity IoT
-

Principali competenze apprese:

Conoscenza dei fondamenti di diritto dell'informatica con particolare attenzione ai risvolti penalistici connessi alla cybersecurity, mediante analisi di singole fattispecie di reato e di illecito, in relazione sia ai reati ordinari che assumono rilievo nelle condotte criminose commesse a mezzo di uno strumento informatico o telematico, sia ai più specifici computer crime introdotti dalla L. 547/1993. Caratteristiche del Cybercrime, e genesi del Cybercrime e Identità Digitale, cenni su transnazionalità del Cybercrime. Analisi degli illeciti contenuti all'interno della L. 633/1941 sul diritto d'autore, L. 48/2008 in esecuzione della Convenzione di Budapest, con relative modifiche al cpp in ordine alla valenza probatoria della prova digitale acquisita secondo le Best practices internazionali della digital forensics, L. 38/2006 sulla pedopornografia, fondamenti di tutela dei dati personali ai sensi del Regolamento europeo 2016/679 e d. lgs. 101/2018.

II.8 Fundamentals of Computer Forensics

Responsabile: Mattia Epifani
Ore: 8
(4 ore Dr. Mattia Epifani, 4 ore Dr. Danilo Massa)

Pre-requisiti:

- Conoscenza di base dei principali file system e sistemi operativi

Programma:

- Digital forensics e digital evidence: definizioni e aspetti tecnici di base
- Le linee guida e le best practices in materia
- Digital Forensics Process Model
- Ordine di volatilità
- Forensic imaging
- Chain of custody
- Digital Forensics & Incident Handling
- NIST sp 800-86 Recommendations
- Enterprise Forensics elements

Principali competenze apprese:

- **Comprendere gli aspetti di base della Digital Forensic**

II.9 Cyber Security in Financial and Credit Systems

Responsabile: Rodolfo Zunino
Ore: 4
(4 ore Dr. Luca Gaudio)

Pre-requisiti:

- Nessuno

Programma:

- Aspetti specific della Cyber security nel settore bancario
- Policy e normativa

Principali competenze apprese:

- Consapevolezza delle specifiche tematiche relative al settore Bancario/Finanziario e loro peculiarità

II.10 Cybersecurity in SCADA Systems, Industry, Power, and Energy

Responsabile: Mario Marchese

Ore: 32

(6 ore Prof. Mario Marchese, 6 ore Dr. Alessio Aceti, 6 ore Ing. Gaetano Sanacore, 6 ore Ing. Micaela Caserza Magro, 6 ore Ing. Gabriele Nani, 2 ore Ing. Lorenzo Ivaldi)

Pre-requisiti:

- Conoscenze di base sulle infrastrutture critiche e sui Protocolli Industriali (TCP/IP based)
- Conoscenza base delle reti industriali (IT/IIoT/OT)
- Basi di ICS and SCADA systems

Programma:

Industrial Networks: Reti di Comunicazione in tempo reale (M. Caserza Magro) – 6 ore)

- I sistemi di automazione
- I protocolli di comunicazione
- Gli standard di riferimento
- Profinet, Profibus

Cybersecurity for Power and Energy (M. Marchese) – 8 ore

- Link to Critical Infrastructures and ICS
- Transmission and Distribution Grid
- ICT model in a transmission system and in a distribution system
- Elements: SCADA and PMU
- Vulnerabilities in power systems
- PMU and Networking, PMU Network as a SCADA Network
- PMU Network as a part of a Smart GRID
- PMU architecture and standards
- Practical example of PMU communications interfaces: Ethernet

Communication, Serial Communication, RS232, RS485, K-BUS

- Available Data Protocols over Ethernet and Serial solutions
- IEEE C37.118-2005
- IEEE C37.118 - Data type format
- Cyber attacks to PMU networks
- Microgrids: control loop and requirements
- Microgrids: vulnerabilities and vectors, Cyber-incidents and Violations
- Impacts of cyberattacks on microgrid operations
- Defense-in-Depth framework enabled by SDN technologies
- Vulnerability assessment in a smart grid
- Major standards for operating a smart grid
- MODBUS: protocol, PDU, function codes
- Operative Examples

Cyber Security of SCADA Systems: Drive effective operations with complete plant information (Nani) – 8 ore

- Overview
- SCADA concept and high level structure
- S+ Operations Overview
- Architecture
- High performance workplace
- Integrated alarm management
- Integrated information management
- Secure operations
- IT vs OT best practices
- Cybersecurity for ABB, position and approach
- ABB cybersecurity in a power plant
- Cybersecurity workplace
- Network Monitoring
- Security patch and anti-virus updates
- Backup and recovery solutions
- Physical hardening
- COC evolution to support SOC features

Cyber defense approach in SCADA/ICS/OT systems for manage the generation/ transmission/ distribution systems (G. Sanacore) – 8 ore

- Cyber Defense approach in Generation/Transmission/Distribution Systems;
- A2A Power Energy Systems Resilience approach;
- Overview to National security Framework – NIS Directive approach;
- Computer Security Incident Response Team(CSIRT) overview - A2A case study;
- Overview to Cybernetic National Security Perimeter (L. n.133);

- Cyber Security compliance for systems/devices procurement;
- ISO/IEC Protocols security suite(CT 57) for Electrical SCADA Systems;
- New IIoT Protocol security suite for Industrial-OT networks;
- Policy for Managing the Electrical Grid Security in SCADA/ICS systems;
- Smart Grid, Power Plants, Transmission & Distribution Grids Cyber Security procedures;
- System security solution & Case study

Cybersecurity and ICS: how can we handle critical infrastructures hacking? (Aceti) – 8 ore

- How did we get involved
- Critical Infrastructures being hacked everyday
- How does it happen?
- What do we learned?
- How can we handle?
- IT and ICS cyber kill chain
- What do you need: patrolling or investigating?
- ICC IoT Security Maturity Model
- Industroyer attack scheme
- Recap
- Assess your SOC
- Alignment to the NIST Cybersecurity framework
- You cannot do it alone
- Virtual CISO
- Ho to disclose cyber incidents?
- Global ICS situation: ransomware, common malware, vulnerabilities
- What to do
- Browser isolation
- Cyber-physical security
- Phased-approach
- Threat Assessment
- Situational Awareness
- Countermeasures
- Operative examples

Principali competenze apprese

- Industrial Networks: solutions and protocols
- Architectures, protocols, vulnerabilities and solutions in Power and Energy systems
- Cyber Security operations driven by complete plant
- Cyber defense approach in generation/distribution systems
- Critical infrastructures hacking Handling