Principali informazioni sull'insegnamento

Denominazione dell'insegnamento	**Analisi e Gestione del Rischio**
Corso di studio	Sicurezza Informatica
Anno Accademico	2025/26
Crediti formativi universitari (CFU) / European Credit Transfer and Accumulation System (ECTS)	6 CFU
Settore Scientifico Disciplinare	SECS-S/01- Statistica
Lingua di erogazione	Italiano
Anno di corso	Primo
Periodo di erogazione	2^ semestre, le date esatte sono riportate nel regolamento dei Corsi di Studio
Obbligo di frequenza	La frequenza è fortemente raccomandata
Sito web del corso di studio	https://www.uniba.it/it/corsi/cdl-sicurezza-informatica-taranto/corso-di-laurea-in-sicurezza-informatica-sede-di-taranto

Docente/i

Nome e cognome	Giovanni Dimauro
Indirizzo mail	giovanni.dimauro@uniba.it
Telefono	+39805443294
Sede	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Stanza n.617, 6^ piano.
Sede virtuale	Piattaforma e-learning di UNIBA - https://elearning.uniba.it/
Sito web del docente	http://www.di.uniba.it/~dimauro/
Ricevimento (giorni, orari e modalità, es. su appuntamento)	Al termine della lezione, ma anche previo appuntamento per email

Syllabus

Obiettivi formativi	Nel corso si tratta la teoria alla base della gestione del rischio sociotecnico incentrata sull'uomo nell'industria di processo con estensione alla sicurezza informatica.

<table>
<tr><td></td><td>Il corso delinea i principi fondamentali della gestione del rischio e come possono essere applicati per apportare miglioramenti concreti nell'identificazione, comprensione, analisi, controllo, comunicazione e governance del rischio. Per massimizzare la competitività sostenibile è necessario identificare e ottimizzare la gamma di rischi che possono avere un impatto su un'azienda.
Nel corso si fa riferimento allo standard internazionale per la gestione del rischio ISO 31000:2018 che definisce il rischio come “l’effetto dell’incertezza sugli obiettivi” o il potenziale di deviazioni positive e negative che creano un’incertezza importante perché può avere un impatto sul raggiungimento degli obiettivi.</td></tr>
<tr><td>Prerequisiti</td><td>- conoscenza della lingua inglese</td></tr>
<tr><td>Contenuti di insegnamento (Programma)</td><td>1) Introduzione al rischio nelle industrie di processo
<table><tr><td>– Introduzione
– Cos'è il rischio?
– Alcuni principi guida
– Casi di studio: alcune conseguenze reali di una gestione inadeguata del rischio (Fonterra, Buncefield, Deepwater Horizon)
– Perché la gestione del rischio è così importante?
– Quali tipi di rischi dovrebbero considerare gli ingegneri?
– Scenari di decisione ingegneristica</td><td>(5h)</td></tr></table>
2) Fondamenti della gestione del rischio
<table><tr><td>– Introduzione
– Il linguaggio del rischio
– Il processo di gestione del rischio
– Chi è responsabile della gestione del rischio?
– Una breve storia della gestione del rischio operativo nel settore</td><td>(5h)</td></tr><tr><td>– Due approcci alla moderna gestione del rischio
– Casi di studio che illustrano due approcci alla gestione del rischio (impianto di processo, DPI di sicurezza)</td><td>(2h)</td></tr></table>
3) Identificare, valutare e trattare i rischi
<table><tr><td>– Introduzione
– Stabilire il contesto
– Valutazione del rischio
– Identificazione del rischio</td><td>(3h)</td></tr></table></td></tr>
</table>

	– Identificazione del rischio, alte tecniche – casi di studio analisi SWOT – Analisi del rischio – Valutazione del rischio – Trattamento e gestione del rischio – Panoramica del trattamento del rischio – Analisi bowtie – Caratterizzazione dell'evento indesiderato – Identificazione dell'evento indesiderato – Determinazione dell'ambito dell'analisi – Identificare le minacce che possono causare l'evento indesiderato	(5h)
	– Identificare le possibili conseguenze che potrebbero derivare dall'evento indesiderato – Analisi del controllo	(5h)
	– Gestione dei controlli	(1h)

4) **Monitorare e rivedere i rischi**

– Introduzione – Perché eseguire indagini sugli eventi? – Scopo e teoria alla base delle indagini – Tecniche di indagine sugli incidenti e considerazioni sull'applicazione – Attenzione utente – Cronologia – Analisi dei 5 perché – Analisi dei fattori umani e sistema di classificazione	(4h)
– Analisi Bowtie – Mappatura dell'analisi degli incidenti – Analisi delle strategie per migliorare la resilienza – Integrazione dell'apprendimento nel business	(5h)

5) **Seminari di approfondimento** (3h)
- Cybersecurity: anatomia di un disastro, Eulogic NT SpA, dr. Claudio Tinelli
- Il valore della Threat Intelligence Strategica nella gestione del rischio cyber, Exprivia S.p.A., dott.ssa Rosita Galiandro
- OT security (Operational Technology Security) - protezione dei sistemi e delle infrastrutture critiche, Techloop, dr. Fabio Marchitelli

6) **Casi di studio (contattare il docente)**
- studio autonomo dei capitoli 11 e 13 del testo e individuazione dei casi di studio personali o di gruppo con utilizzo della tecnica Bowtie e CAMS
- tracce di altri casi di studio sono riportate nell'apposita sezione della piattaforma elearning

Testi di riferimento	**Testo adottato:** Fundamentals of risk management for process industry engineers

	Maureen Hassall and Paul Lant Elsevier, 2023 ISBN: 978-0-12-820320-0 **Materiale base per studiare (riferimento alla sezione precedente)**: – Slide del corso fornite dal docente – ISO-31000 (PDF) – Esempio Analisi SWOT (PDF) – Cyber - Using Bow Tie Risk Modeling for Industrial Cybersecurity Whitepaper - Dragos OSIsoft 2021 (PDF) – The first 100 days of the Information Security Manager (PDF) **Materiale facoltativo**: – Texas – 5 why – CSBFinalReportBP (PDF) – The fifth age of security – The adaptive age (PDF) – A white paper on cybersecurity (PDF) – Tecnica HAZOP (PDF) Gli studenti che lo desiderano possono ottenere i testi in prestito dalla Biblioteca. Può convenire verificarne la disponibilità mediante il Sistema Bibliotecario di Ateneo https://opac.uniba.it/easyweb/w8018/index.php? e contattare la biblioteca per concordare il prestito.
Note ai testi di riferimento	Il materiale per lo studio, già presentato a lezione, è integralmente indicato alla sezione precedente. Per lo svolgimento dei progetti, il docente può fornire ulteriore materiale in base al tipo di progetto scelto dallo studente. Gli studenti non frequentanti possono prendere contatto per email con il docente per chiarimenti, per concordare il progetto e le modalità d'esame.

Organizzazione della didattica

Ore

Totali	Didattica frontale	Laboratorio	Studio individuale
150 ore	48 ore		102 ore

CFU/ETCS

6 CFU	6 CFU		

Metodi didattici

	Lezioni frontali, esercitazioni ed attività autonome e di gruppo in aula e a casa. Gli studenti non frequentanti possono lavorare singolarmente prendendo accordi con il docente.

Risultati di apprendimento previsti	
Conoscenza e capacità di comprensione	• Acquisire conoscenze che consentano allo studente di comprendere quali sono le problematiche in ambito di Analisi e Gestione del Rischio nelle industrie di Processo e in generale di rischio informatico e quali le possibili soluzioni.
Conoscenza e capacità di comprensione applicate	• Comprendere quali sono le caratteristiche organizzative e operative di un'azienda per affrontare il rischio.
Competenze trasversali	**Autonomia di giudizio** • Acquisire la capacità di verificare se un'azienda è ben organizzata e opera attivamente per la prevenzione del rischio; **Abilità comunicative** • Imparare a commentare le soluzioni prodotte al fine di renderle comprensibili e agevolmente utilizzabili da professionisti di altri settori. **Capacità di apprendere in modo autonomo** • Capacità di interagire con esperti e acquisire le esigenze molto specifiche di un settore con particolari esigenze di affidabilità, tempestività, integrabilità e coerenza con i normali processi di analisi e gestione del rischio.

Valutazione	
Modalità di verifica dell'apprendimento	Per sostenere l'esame è necessario studiare dal testo di riferimento e dal materiale messo a disposizione dal docente e sviluppare un progetto (preferibilmente in gruppo) o una tesina concordati con il docente. L'impegno e il tempo stimati per preparare il progetto/tesina è commisurato ai CFU dell'insegnamento ed è tale da consentire allo studente di sostenere l'esame già al primo appello di giugno); si suggerisce pertanto allo studente di impegnarsi allo svolgimento del progetto già nel corso delle lezioni, con coda (breve in termini temporali) prima dell'esame. Esempi di casi di studio/tesina possono essere chiesti al docente anche per email. L'esame finale consiste nella discussione del progetto o della tesina e nella prova orale sui temi del corso. La prova orale potrà essere organizzata in forma colloquiale o di test a risposta multipla. Non sono previste prove di valutazione intermedia (cd esoneri). Le prove (orale - progetto/tesina) possono essere sostenute nell'ordine che lo studente preferisce.

<table>
<tr><td></td><td>Tipo di valutazione: voto in trentesimi.

Incentivi alla frequenza: L'eventuale lode potrà essere attribuita soprattutto agli studenti che per la stragrande maggioranza delle lezioni hanno frequentato, interagito nel corso della lezione, proposto soluzioni e risolto i casi proposti dal docente a lezione.

Eventuali materiali utili per sostenere la prova: documentazione e/o software prodotti dallo studente.

Modalità di comunicazione dei risultati della prova: in presenza.</td></tr>
<tr><td>Criteri di valutazione</td><td>• Conoscenza e capacità di comprensione:
○ Lo studente dovrà essere in grado di analizzare e descrivere problemi nell'ambito dei contenuti del corso.

• Conoscenza e capacità di comprensione applicate:
○ Lo studente dovrà essere in grado di analizzare una situazione e formulare un piano di gestione del rischio;
○ Lo studente dovrà essere in grado di utilizzare un ambiente di sviluppo a sua scelta;

• Autonomia di giudizio:
○ Lo studente dovrà essere in grado di correggere e validare la corretta formulazione di un piano di gestione del rischio.

• Abilità comunicative:
○ Lo studente dovrà essere in grado di descrivere le problematiche generali previste nel corso e descrivere e documentare le applicazioni implementate.

• Capacità di apprendere:
○ Lo studente dovrà essere in grado di spiegare come le conoscenze e competenze acquisite le utilizzerebbe per risolvere problemi analoghi ai settori applicativi oggetti del corso.</td></tr>
<tr><td>Criteri di misurazione dell'apprendimento e di attribuzione del voto finale</td><td>
<table>
<tr><th>Voto</th><th>Descrittori</th></tr>
<tr><td>< 18 insufficiente</td><td>Conoscenze frammentarie e superficiali dei contenuti, errori nell’applicare i concetti, descrizione carente.</td></tr>
<tr><td>18 - 20</td><td>Conoscenze dei contenuti sufficienti ma generali, descrizione semplice, incertezze nell’applicazione di concetti teorici.</td></tr>
<tr><td>21 - 23</td><td>Conoscenze dei contenuti appropriate ma non approfondite, capacità di applicare i concetti teorici, capacità di presentare i contenuti in modo semplice.</td></tr>
<tr><td>24 - 25</td><td>Conoscenze dei contenuti appropriate ed ampie, discreta capacità di applicazione delle conoscenze, capacità di presentare i contenuti in modo articolato.</td></tr>
<tr><td>26 - 27</td><td>Conoscenze dei contenuti precise e complete, buona capacità di applicare le conoscenze, capacità di analisi, descrizione chiara e corretta.</td></tr>
<tr><td>28 - 29</td><td>Conoscenze dei contenuti ampie, complete ed approfondite, buona applicazione dei contenuti, buona capacità di analisi e di sintesi, descrizione sicura e corretta.</td></tr>
</table>
</td></tr>
</table>

30 30 e lode	Conoscenze dei contenuti molto ampie, complete ed approfondite, capacità ben consolidata di applicare i contenuti, ottima capacità di analisi, di sintesi e di collegamenti interdisciplinari, padronanza di descrizione.

Altro

Si suggerisce agli studenti di affidarsi esclusivamente alle informazioni/comunicazioni fornite sui siti ufficiali del Dipartimento di Informatica, ovvero sui gruppi social solo se costituiti e amministrati esclusivamente dai docenti dei relativi insegnamenti:

- https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea
- https://www.uniba.it/it/ricerca/dipartimenti/informatica
- https://elearning.di.uniba.it/

I programmi degli insegnamenti sono disponibili qui:
- https://elearning.uniba.it/course/index.php?categoryid=104

Le informazioni che tutti gli studenti dovrebbero conoscere sono scritte nei Regolamenti didattici e manifesti degli studi disponibili nel sito:
- https://www.uniba.it/it/corsi/cdl-sicurezza-informatica-taranto/corso/scheda-del-corso/scheda-cds-sicurezza-informatica

Si suggerisce agli studenti di diffidare delle informazioni e dei materiali circolanti su siti o gruppi social non ufficiali, poiché spesso sono risultati non affidabili, non corretti o incompleti. Per ogni dubbio, chiedere un incontro al docente secondo le modalità previste per il ricevimento.

Si suggerisce agli studenti di unirsi al forum del corso su Telegram, utilizzato per scopi didattici e di collaborazione tra studenti, al quale aderisce anche il docente: https://t.me/+nLxJwU2l9Ps0Njg0