# Tecnologie per la sicurezza

## Prof. Marika Assogna; Prof. Franco Fantozzi

I Modulo: *Sicurezza degli ambienti informatici* (Prof. Marika Assogna)

***OBIETTIVO DEL CORSO E RISULTATI DI APPRENDIMENTO ATTESI***

Ogni azienda dispone di un patrimonio informativo costituito dai dati elettronici che vengono scambiati o elaborati mediante il supporto di strumenti e processi tecnologici (ICT). Questi dati sono essenziali per le attività di business che l’azienda conduce e pertanto devono essere protetti adeguatamente garantendone riservatezza, integrità e disponibilità.

La mancanza di adeguati livelli di sicurezza delle informazioni può generare effetti negativi per l’azienda, anche in termini di sanzioni legate alla violazione delle normative vigenti che dettano prescrizioni relativamente ai sistemi e ai processi ICT (ad es. GDPR, PSD2, DORA, EBA Guidelines). Pertanto, la sicurezza dei processi e delle informazioni in ambito ICT riveste un ruolo essenziale nell’ottica dell’operatività aziendale e può essere ottenuta implementando opportune misure di sicurezza per ridurre i rischi cui risulta esposto il patrimonio informativo nel suo complesso.

L’insegnamento si propone di fornire allo studente l’indirizzo generale da seguire al fine di comprendere come tutelare e proteggere le informazioni e i processi operativi di business aziendali nello specifico ambito ICT, sia dal punto di vista della continuità operativa del business che dal punto di vista del governo del rischio e della compliance ICT.

Scopo dell’insegnamento è che i partecipanti acquisiscano conoscenze sulle principali normative e standard di settore che definiscono importanti indicazioni sulle misure organizzative e tecniche da intraprendere, in un’azienda, per poter gestire la sicurezza informatica. Il corso si dividerà in due parti: la prima con nozioni di carattere teorico e la seconda con workshop dove verranno richieste soluzioni a casi reali di aziende che presentano problematiche di sicurezza informatica.

La struttura del corso è data da un continuo intrecciarsi di momenti puramente teorici con esercizi pratici svolti in aula e con il supporto del docente.

Al termine dell’insegnamento, lo studente sarà in grado di conoscere le principali minacce di sicurezza informatica e acquisirà dimestichezza con i processi ICT.

Lo studente sarà in grado di indentificare i rischi e le vulnerabilità connesse ai sistemi ICT e definire i requisiti di sicurezza ICT necessari per la tutela delle informazioni aziendali.

Lo studente sarà altresì in grado di esaminare i principali requisiti normativi in tema di ICT security compliance e di applicarli a casi concreti.

***PROGRAMMA DEL CORSO***

1*. Nozioni teoriche*

Gestione del Rischio ICT e di sicurezza informatica.

Che cos’è un sistema IT e come è composto: nozioni base.

Il ciclo Plan-Do-Check-Act.

ITIL-IT Service Management.

Lo standard ISO/IEC 27001:2022 -

*Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (Controlli organizzativi, Politica per la sicurezza ICT; Organizzazione per la sicurezza delle informazioni (cenni) Separazione dei ruoli, Controlli sulle risorse umane (cenni), Gestione dei beni; Controllo Accessi, Crittografia, Controlli per la sicurezza fisica ed ambientale (cenni), Controlli tecnologici, Gestione operations; Gestione delle comunicazioni; Acquisizione, sviluppo e manutenzione dei sistemi informativi; Relazioni con i fornitori, Gestione degli incidenti della sicurezza delle informazioni; Aspetti di sicurezza informatica nella gestione della continuità delle attività aziendali; Conformità ed Audit).

Sistema di Controllo Interno: le attività di controllo e il rischio di non conformità: focus su risk & compliance ICT.

Principi specifici introdotti dal Regolamento Europeo per la Protezione dei dati personali (GDPR) correlati alla sicurezza ICT: privacy by design e by default; *Data Protection Impact Assessment* (DPIA); data breach (notifica e comunicazione al Garante).

Le principali minacce informatiche: definizioni, cause, modalità di esecuzione e contromisure di sicurezza.

2*. Workshop*

Presentazione di casi concreti di varie aziende con diverse problematiche relative alla sicurezza informatica. Discussione e lavoro in gruppo per fornire la migliore soluzione al caso.

***BIBLIOGRAFIA[[1]](#footnote-1)***

La bibliografia sarà presentata dal docente all’inizio delle lezioni e sarà disponibile su Blackboard.

***DIDATTICA DEL CORSO***

Lezioni in aula, discussioni collettive, lavoro in gruppi durante i workshop, elaborazione di paper singoli o di gruppo e presentazione e discussione dei risultati delle esercitazioni.

***METODI E CRITERI DI VALUTAZIONE***

L'esame è in forma scritta e si svolge in aula informatica con l’ausilio di un pc. La prova si divide in due parti. Nella prima parte lo studente deve rispondere a 20 domande a risposta multipla. Le domande a risposta multipla sono corrette subito dal sistema e lo studente conoscerà immediatamente il voto. Nella seconda parte lo studente deve rispondere a 3 domande aperte. Le risposte date saranno corrette dal docente in seguito alla conclusione dell’esame. Il docente valuterà le domande aperte in base all’esatta comprensione della domanda, ivi compreso l’utilizzo di una corretta sintassi grammaticale nella risposta, ed alla capacità dello studente di sviluppare opportuni collegamenti ad altri argomenti del programma corredandoli con esempi pratici.

Il voto della prova è determinato dalla somma dei punteggi totalizzati nelle due parti.

***AVVERTENZE E PREREQUISITI***

Avendo carattere introduttivo, l’insegnamento non necessita di prerequisiti relativi ai contenuti. Si presuppone comunque interesse e curiosità per le tecnologie e una sensibilità alla valutazione dei rischi.

Nel caso in cui la situazione sanitaria relativa alla pandemia di Covid-19 non dovesse consentire la didattica in presenza, sarà garantita l’erogazione a distanza dell’insegnamento e degli esami di profitto, con modalità che verranno comunicate in tempo utile agli studenti.

*Orario e luogo di ricevimento*

Il Prof. Marika Assogna riceve gli studenti su appuntamento inviando una mail a *marika.assogna@gmail.com.*

II Modulo: *Sicurezza degli ambienti fisici* (Prof. Franco Fantozzi)

***OBIETTIVI DEL CORSO E RISULTATI DI APPRENDIMENTO ATTESI***

Il processo di security aziendale rappresenta il complesso delle attività di valutazione, gestione, controllo e riesame dei rischi e delle minacce e deve essere gestito dal professionista della security.

Scopo delle attività di security è quello di prevenire, fronteggiare e superare eventi, che possano colpire le risorse materiali, immateriali, organizzative ed umane di cui l’azienda dispone

Il security manager dovrà quindi disporre delle conoscenze, competenze ed abilità necessarie per svolgere efficacemente il proprio ruolo.

L’obiettivo del corso sarà quindi fornire ai futuri professionisti della security aziendale gli strumento tecnici, normativi e soprattutto metodologici per sviluppare le conoscenze, le abilità e le competenze richieste per il corretto svolgimento della propria funzione.

L’attuale modello di security, focalizzato non più e non solo sui beni aziendali da proteggere, si concentra sui rischi e le minacce che possono influire negativamente sul business e sulla continuità della produzione o del servizio.

Verranno pertanto sviluppati aspetti relativi alla metodologia per la corretta individuazione, analisi e mitigazione del rischio e per la realizzazione di un piano di security. Saranno poi approfonditi gli elementi della gestione di una crisi aziendale e del ruolo del security manager all’interno del crisis team.

Il modulo si concentrerà infine sui contenuti dell’attività investigativa, della sicurezza del personale in trasferta e della sicurezza della catena logistica, senza tralasciare gli aspetti di privacy e di normative internazionali.

Al termine dell’insegnamento, lo studente sarà in grado di effettuare autonomamente il processo di identificazione, analisi e gestione dei rischi di security e di individuare le misure di mitigazione dello stesso, sia in ambito sicurezza fisica e sia in ambito sicurezza della catena logistica.

Lo studente, anche attraverso una simulazione di scenario, conoscerà le fasi, il processo e la metodologia di approccio alla gestione degli eventi critici e si avvicinerà alla gestione del travel risk management in modo olistico, apprendendo gli elementi fondamentali per una corretta pianificazione e gestione del rischio trasferta.

***PROGRAMMA DEL CORSO***

1. La security aziendale.

Evoluzione della figura di security manager, la Norma UNI 10459, Profili professionali, conoscenze e competenze.

1. Risk management e security risk management. Analisi del rischio secondo lo standard ISO 31000:2018 e realizzazione di un piano di security.
2. Crisis management ed elementi di Business Continuity management.

Analisi della crisi. Esame delle best e worst practices in ambito gestione della crisi, il Crisis team e la gestione della crisi;

Esercitazione su gestione della crisi e delle emergenze. Simulazioni di scenario; linee guida per la realizzazione di un piano di continuità operativa;

1. Tutela della privacy e security.

Video sorveglianza ed utilizzo di sistemi informatici nell’attività di controllo dei lavoratori. Il regolamento europeo GDPR sulla tutela dei dati personali. Modello organizzativo 231/2001; strumenti di controllo dei lavoratori e rispetto della privacy;

1. Supply chain security.

Cargo crime. La sicurezza nella catena di trasporto e distribuzione dei beni. I programmi di sicurezza e gli standard TAPA, CT-PAT, AEO. La security nel retail ed il last mile. La Norma ISO 28000:2007. Site security assessment;

1. Travel risk management.

Tutela e gestione operativa del capitale umano in trasferta. Presenza occasionali all’estero ed EXPAT, la responsabilità penale dell’impresa; il duty of care, la norma ISO 31030:2021 sul travel risk management, la travel risk policy e la sicurezza personale in trasferta.

Case studies.

Review degli insegnamenti svolti e preparazione all’esame.

***BIBLIOGRAFIA[[2]](#footnote-2)***

Slides e presentazioni fornite dal docente;

Ricerche ipertestuali su siti indicati dal docente e consultazioni di documenti ufficiali;

“Security risk management”, autore: Stefano BONACINA, IPSOA editore, 2010;

“La perfetta comunicazione d’emergenza, autore: Mauro de Vincentis, Editori di comunicazione-Lupetti, 2001;

“Crisis therapy” autore: Andrea Polo, edizioni Il Sole 24 ore;

“Manuale di Business continuity e crisis management”, autore: Anthoiny Cecil Wright, Franco Angeli editore;

“Governare il rischio. Un modello di security risk management”, autore: Umberto Saccone, edizioni ARACNE, 2014;

“Gè-Politikè”, Manuale di introduzzione alla analisi geopolitica, autore: Stefano Cont, Laurus Robuffo;

GDPR e Decreto Legislativo 101/2018, a cura di Marco Martorana, Wolters Kluver;

Risk Managenent, la norma ISO 31000: 2018, di Ioannis Tsiouras, edizioni Youcanprint;

***DIDATTICA DEL CORSO***

Il corso è caratterizzato da lezioni frontali con ampia interazione verso gli studenti e partecipazione attiva alla disamina e valutazione di case studìes ed esempi pratici. Nel corso della simulazione di gestione della crisi verranno prodotti documenti e si procederà con un esame di gruppo dei risultati del test. Ulteriore esercitazione sarà focalizzata sulla impostazione di un security plan.

***METODO E CRITERI DI VALUTAZIONE***

L'esame è in forma scritta e la prova si divide in due parti. Nella prima parte lo studente deve rispondere a 20 domande a risposta multipla, assegnate in maniera casuale tra le 100 proposte dal docente. Le domande a risposta multipla sono corrette subito dal sistema e lo studente apprende immediatamente il voto. Nella seconda parte lo studente deve rispondere a 3 domande aperte, assegnate in manierra casuale tra le 20 proposte dal docente. Le risposte date saranno successivamente corrette dal docente il quale valuterà le domande aperte con un punteggio massimo di 4 punti.

Gli studenti, nel corso della prova scritta, dovranno dimostrare l’esatta comprensione della domanda, la capacità di sviluppare collegamenti con altri argomenti del corso calandoli nel contesto della domanda stessa ed utilizzando una corretta sintassi grammaticale nella risposta.

Sarannoi altresì in grado di riportare nella loro dissertazione scritta gli esempi pratici ed i collegamenti con casi reali sviluppati durante le lezioni.

Il voto della prova è determinato dalla somma dei punteggi totalizzati nelle due parti

***AVVERTENZE E PREREQUISITI***

La frequenza al corso, seppur non obbligatoria, è fortemente raccomandata.

Le slides ed il materiale integrativo, utile per la preparazione all’esame, sarà reso disponibile on line.

Pur non richiedendo prerequisiti particolari relativi ai contentui, ai fini di una efficace e proficua interazione, l’insegamento della security intesa come attività volta a prevenire, fronteggiare e superare eventi che possano esporre le persone ed i beni (materiali ed immateriali) di una Organizzazione a effetti lesivi e/o dannosi richiede interesse per le materie di carattere giuridico e spiccata curiosità intelletutale verso la crescente complessità degli scenari economico-produttivi e geo-politici.

*Orari e luogo di ricevimento*

Il Prof. Franco Fantozzi riceve gli studenti solamente su appuntamento inviando una mail a franco.fantozzi@unicatt.it o ffantozzi9@gmail.com, con almeno 7 giorni di preavviso.

Se rischiesto, il docente è disponibile ad incontri on line per l’approfondimento di specifiche tematiche.

1. I testi indicati nella bibliografia sono acquistabili presso le librerie di Ateneo; è possibile acquistarli anche presso altri rivenditori. [↑](#footnote-ref-1)
2. I testi indicati nella bibliografia sono acquistabili presso le librerie di Ateneo; è possibile acquistarli anche presso altri rivenditori. [↑](#footnote-ref-2)