# 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, Circolare Bankit 285). 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*

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 27001:2013 - *Information technology - Security techniques - Information security management systems - Requirements* (Politica per la sicurezza ICT; Organizzazione per la sicurezza delle informazioni (cenni), Sicurezza delle risorse umane (cenni), Gestione dei beni; Controllo Accessi, Crittografia, Sicurezza fisica ed ambientale (cenni), 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 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)

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

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

Il security manager dovrà quindi disporre delle conoscenze, competenze ed abilità necessarie per svolgere efficacemente il ruolo di responsabile della sicurezza.

L’obiettivo del corso sarà quindi fornire ai futuri professionisti della security aziendale o ai futuri operatori della sicurezza pubblica, 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, denominato “total risk governance”, 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 governance dei rischi e delle minacce, con riferimenti concreti ed esempi inerenti alla gestione della crisi e l’integrazione della funzione di security manager nel processo a sostegno e supporto del business aziendale.

***PROGRAMMA DEL CORSO***

1. La security aziendale.

Evoluzione della figura di security manager, la Norma UNI 10459, Profili professionali, gestione del rischio in azienda;

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. Role playing;

3. 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;

4. Sicurezza fisica.

Controllo degli accessi e vigilanza. Protezione attiva e passiva delle infrastrutture. Tutela della salute e sicurezza nei luoghi di lavoro di cui al D.Lgs. 81/2008;

Esercitazione sull’elaborazione di un piano di security

5. 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 e la ISO 31000:2018.

7. Travel risk management.

Tutela e gestione operativa del capitale umano delocalizzato. Presenza occasionali all’estero ed EXPAT, la responsabilità penale dell’impresa; il duty of care.

Case study.

8. 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;

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

“Manuale di sicurezza aziendale. Proteggere i beni materiali e immateriali nelle aziende e nelle Istituzioni”. Avigliano Umbro edizioni, 2013;

“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;

Esplorare Internet, Manuale di OSINT, autore: Leonida Reitano, MINERVA;

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 study ed esempi pratici. Nel corso del role playing di simulazione di gestione della crisi verranno prodotti documenti e si procederà con l’esame di gruppo dei risultati dell’esercitazione. 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 successivamnete corrette dal docente il quale valuterà le domande aperte in base all’esatta comprensione della domanda, alla capacità di sviluppare collegamenti con altri argomenti del corso calandoli nel contesto della domanda stessa ed all’utilizzo di una corretta sintassi grammaticale nella risposta..

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

***AVVERTENZE E PREREQUISITI***

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.

*Orari e luogo di ricevimento*

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

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)