



UNIVERSITÀ DI PISA

ORGANIZZAZIONE AZIENDALE E SISTEMI INFORMATIVI

FEDERICO NICCOLINI

Anno accademico 2020/21
CdS STRATEGIA, MANAGEMENT E CONTROLLO
Codice 379PP
CFU 6

Moduli	Settore/i	Tipo	Ore	Docente/i
ORGANIZZAZIONE AZIENDALE E SISTEMI INFORMATIVI	SECS-P/10	LEZIONI	42	FEDERICO NICCOLINI

Obiettivi di apprendimento

Conoscenze

Il corso ha il fine di migliorare le conoscenze degli studenti in merito agli strumenti e alle metodologie per la corretta analisi e implementazione dei sistemi informativi nel contesto organizzativo. Lo studente acquisirà, in particolare, conoscenze rispetto agli ai sistemi e strumenti di Information Technology che maggiormente impattano sulla performance ed efficacia delle organizzazioni, come i sistemi CRM o ERP. Particolare attenzione sarà assegnata allo sviluppo di conoscenze e abilità con riferimento ai temi dei big data e della cybersecurity.

Modalità di verifica delle conoscenze

Per l'accertamento delle conoscenze, all'inizio di ogni lezione sarà richiesto agli studenti un rapido feedback (di circa 5-10 minuti) sui concetti cardine lezione precedente. Saranno fatti anche dei rapidi test su concetti chiave (usando ad esempio lo strumento Polly). La verifica delle conoscenze sarà poi oggetto della valutazione dell'elaborato scritto previsto all'inizio di ogni appello d'esame

Capacità

Al termine del corso lo studente avrà acquisito gli strumenti per interpretare le caratteristiche dei sistemi informativi in relazione a quelle del contesto organizzativo. Il corso si propone, inoltre, di arricchire le capacità degli studenti in termini di lavoro di gruppo, di analisi, di revisione critica di documenti tecnici e casi aziendali e di presentazione in pubblico, con particolare riguardo ai profili dei sistemi informativi in relazione alle variabili organizzative.

Modalità di verifica delle capacità

La verifica delle capacità sarà effettuata anche attraverso un processo di coaching, mentoring e più in generale un approccio di apprendimento partecipativo con cui sono impostate le attività in aula. Al riguardo, gli studenti potranno svolgere dei lavori di gruppo, preparando e mostrando in aula alcune presentazioni aventi ad oggetto temi e casi di studio ritenuti esemplari.

Comportamenti

Lo studente potrà acquisire e sviluppare anche competenze comportamentali interpersonali di lavoro collaborativo ed individuali di public speaking, anche attraverso la partecipazione a lavori di gruppo e la presentazione in aula dei risultati.

Modalità di verifica dei comportamenti

Durante lo svolgimento del corso saranno verificati i comportamenti, osservando le modalità di svolgimento dei lavori di gruppo e, al termine degli stessi, saranno, invece, verificate le modalità di ricerca dei contenuti e di analisi degli argomenti. Presidiando la preparazione e l'esposizione delle presentazioni sarà, poi, possibile verificare le modalità di interpretazione dei casi di studio e di presentazione dei risultati.

Prerequisiti (conoscenze iniziali)

Si ritiene utile che lo studente possieda preliminarmente conoscenze di tipo organizzativo, con particolare riferimento ai concetti di struttura, strategia, tecnologia, conoscenza, cultura organizzative.

Indicazioni metodologiche

Il corso avrà inizio con una serie di lezioni frontali. In seguito, sarà usato un approccio didattico orientato all'apprendimento partecipativo e



UNIVERSITÀ DI PISA

generativo. Le lezioni frontali si alterneranno quindi con lavori di gruppo ed alcuni seminari. Le lezioni frontali saranno svolte con l'ausilio di slide e filmati. Le diapositive di sintesi saranno immesse sulla pagina docente al termine di ogni settimana di lezione. Il docente riceverà gli studenti secondo un orario comunicato a lezione e sulla propria pagina web. Gli studenti potranno contattare il docente anche attraverso l'indirizzo istituzionale di posta elettronica.

Programma (contenuti dell'insegnamento)

I principali contenuti dell'insegnamento sono:

- Risposte organizzative per la cybersecurity
- Web Information System. E-business
- Sistemi Enterprise Resource Planning (ERP)
- Sistemi Customer Relationship Management (CRM)
- Piattaforme di Business Intelligence & Sistemi di supporto alle decisioni (DSS): Management Information Systems, Executive Information Systems
- Big data e relative strutture organizzative per la gestione
- Supply Chain Management
- Knowledge management
- Apprendimento organizzativo

Bibliografia e materiale didattico

1) Daft R. (2017), *Organizzazione aziendale*, Maggioli, Milano, Capitolo 8 (pagg. 288-326)

+ Daft R. (2014), *Organizzazione aziendale*, Maggioli, Milano, Capitolo 8 (pagg. 281-318)

Oppure

+ Daft, R. (2020), *Organization theory and design*. Cengage learning (13th Ed), Chapter, 9 (pp. 360-397)

2) Nonaka I. (2007, July-August), *The knowledge creating company*, Harvard Business Review, pp. 162-166

3) McAfee, A., & Brynjolfsson, E. (2012). *Big data: la rivoluzione manageriale*. Harvard Business Review Italia

4) AA.VV. (2018), *Organizzazione aziendale e sistemi informativi A.A.2018-19*, Progetto Create McGraw-Hill Libri Italia, Milano, ISBN: ISBN 9781307346282 =

- Bracchi G., Francalanci C., & Motta G. (2010), *Sistemi informativi d'impresa*, McGraw-Hill Libri Italia, Milano, Capitoli 1, 3, 4, 5, 6, 9
- Chase R., Jacobs R., Grando A., Sianesi A. (2011), *Operations Management nella produzione e nei servizi*, McGraw-Hill Libri Italia, Milano, Capitoli 10 e 12

5) Kreitner R., Kinicki A., *Comportamento Organizzativo*. Dalla teoria all'esperienza, Apogeo, Milano, 2013, Capitoli 12, 14, solo pagine 257-261 (Team virtuali ed autogestiti), 341-346 (L'impatto della comunicazione digitale sul comportamento organizzativo)

6) Carlton, M., Levy, Y., & Ramim, M. M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information and Computer Security*, 27(1), 101-121. <https://doi.org/10.1108/ICS-11-2016-0088>

National Institute of Standards and Technology (2018a). *Cybersecurity framework*. <https://www.nist.gov/cyberframework>

Paananena, H., Lapkeb, M., & Siponena, M. (2020). State of the art in information security policy development. *Computer & Security*, 101608. <https://doi.org/10.1016/j.cose.2019.101608>

Radichel, T. (2014). Case study: Critical controls that could have prevented target breach. SANS Institute Information Security Reading Room, 1-30.

Letture consigliate

Ross, J.W., Beath, C.M., & Quaadgras, A. (2013). Alla fine, forse, i big data non vi servono. *Harvard Business Review Italia*, dicembre, pp. 53-59

Chulkov, D. V. (2017). Escalation of commitment and information security: Theories and implications. *Information & Computer Security*, 25(5), 580-592. <https://doi.org/10.1108/ICS-02-2016-0015>

International Organization for Standardization (2018). *Information security management (overview)*. <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>

National Institute of Standards and Technology (2018b). *Cybersecurity framework 1.1 - An introduction to the components of the framework*. <https://www.nist.gov/cyberframework/online-learning/components-framework>

Ramim, M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. *Journal of Cases on Information Technology*, 8(4), 24-34. <https://doi.org/10.4018/jcit.2006100103>

Indicazioni per non frequentanti

Gli studenti non frequentanti devono attenersi scrupolosamente al programma indicato.

Spiegazione programma

1)

Daft R. (2017), *Organizzazione aziendale*, Maggioli, Milano, Capitolo 8 (pagg. 288-326)

+ Daft R. (2014), *Organizzazione aziendale*, Maggioli, Milano, Capitolo 8 (pagg. 281-318)

Oppure

+ Daft, R. (2020), *Organization theory and design*. Cengage learning (13th Ed), Chapter, 9 (pp. 360-397)

Occorre studiare questo capitolo in versione "evolutivo/dinamica": lo scopo è comprendere i **cambiamenti** rapidi che ci sono anche nella teoria e nella prassi aziendale in questo campo di studio. Quindi vanno studiate entrambe le versioni. Apparentemente sono 60 pagine, ma in realtà sono circa **45** perché circa 15 si riferiscono ad argomenti comuni.

2) Nonaka I. (2007, July-August), *The knowledge creating company*, Harvard Business Review, pp. 162-166. Queste **5** pagine servono per riportare il campo di studio al tema del **knowledge management**.

3) McAfee, A., & Brynjolfsson, E. (2012). *Big data: la rivoluzione manageriale*. Harvard Business Review Italia, Ottobre, pp. 15-22



UNIVERSITÀ DI PISA

Queste 7 pagine sono per vedere come un tema di particolare attualità nel campo di studio (big data) è affrontato su riviste di settore.

4) AA.VV. (2018), *Organizzazione aziendale e sistemi informativi A.A.2018-19*, Progetto Create McGraw-Hill Libri Italia, Milano, ISBN: ISBN 9781307346282 =

= Bracchi G., Francalanci C., & Motta G. (2010), *Sistemi informativi d'impresa*, McGraw-Hill Libri Italia, Milano, Capitoli 1, 3, 4, 5, 6, 9 +

+ Chase R., Jacobs R., Grando A., Sianesi A. (2011), *Operations Management nella produzione e nei servizi*, McGraw-Hill Libri Italia, Milano, Capitoli 10 e 12

Sono 8 capitoli presi in 2 libri di testo. Non occorre comprare i 2 libri. Essendo i due libri della stessa casa editrice, la stessa ha stampato un così detto Progetto "create": un libro che contiene solo i 7 capitoli selezionati.

Il libro è disponibile sulla seguente pagina di Amazon

- https://www.amazon.it/s?k=9781307346282&__mk_it_IT=%C3%85M%C3%85C5%BD%C3%95%C3%91&ref=nb_sb_noss

5) Kreitner R., Kinicki A., *Comportamento Organizzativo. Dalla teoria all'esperienza*, Apogeo, Milano, 2013, Capitoli 12, 14, solo pagine 257-261 (Team virtuali ed autogestiti), 341-346 (L'impatto della comunicazione digitale sul comportamento organizzativo).

Queste 10 pagine servono per capire la rilevanza del campo di studio nel comportamento organizzativo.

6) Carlton, M., Levy, Y., & Ramim, M. M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information and Computer Security*, 27(1), 101-121. <https://doi.org/10.1108/ICS-11-2016-0088>

National Institute of Standards and Technology (2018a). *Cybersecurity framework*. <https://www.nist.gov/cyberframework>

Paananena, H., Lapkeb, M., & Siponena, M. (2020). State of the art in information security policy development. *Computer & Security*, 101608. <https://doi.org/10.1016/j.cose.2019.101608>

Radichel, T. (2014). Case study: Critical controls that could have prevented target breach. SANS Institute Information Security Reading Room, 1-30.

Gli articoli inquadrano il tema della cybersecurity in chiave organizzativa

Modalità d'esame

La verifica finale è composta da una prova scritta ed una prova orale.

La prova scritta è composta di norma da un numero variabile da 2 a 4 domande, solitamente di tipo aperto. Ad ognuna delle domande aperte è assegnato un punteggio massimo di 8 -16 punti. Il totale dei punteggi acquisibili con lo scritto varia dai 30 ai 33 punti. La prova scritta è superata se lo studente acquisisce una votazione complessiva superiore a 16 punti.

La prova scritta si svolgerà in un'aula normale e mediamente dura 1 ora e 15/20 minuti.

La prova scritta è valida solo per l'appello in cui è stata sostenuta. Al riguardo, l'annotazione sul libretto dello studente e la verbalizzazione deve essere effettuata entro la conclusione dell'appello. L'appello viene chiuso il giorno stabilito per l'orale. Qualora lo studente non si presenti il giorno stabilito per l'orale per la registrazione del voto dello scritto, il voto viene considerato rifiutato e dunque lo studente dovrà sostenere di nuovo l'esame.

La prova orale consiste in un colloquio tra il candidato e il docente ed ha una durata media di 10/20 minuti. La prova orale può aumentare o diminuire il voto dello scritto fino ad un massimo di 5 punti.

La prova non è superata se il candidato mostra di non essere in grado di esprimersi in modo chiaro, di usare la terminologia corretta e manifesta lacune su aspetti contenuti nel programma del corso.

Gli studenti che abbiano svolto lavori di gruppo durante il corso, non dovranno ripresentare l'argomento (preventivamente concordato con il docente) del lavoro di gruppo alla prova di esame, nel caso in cui la votazione ricevuta per il lavoro di gruppo sia pari o superiore a 30/30. Il voto del lavoro di gruppo sarà ponderato per una percentuale (comunicata prima dello svolgimento del lavoro) variabile tra il 15 e il 30% rispetto al voto della prova scritta.

Note

Per la spiegazione della struttura del programma si veda le indicazioni per i non frequentanti

Il Libro create è acquistabile su Amazon alla seguente pagina

https://www.amazon.it/s?k=9781307346282&__mk_it_IT=ÅMÄŽÕÑ&ref=nb_sb_noss

Ultimo aggiornamento 24/09/2020 13:13