

# Cyber security

**Docenti: Barbara Indovina, Michele Slocovich**

## Lingua

Italiano

## Descrizione del corso e obiettivi

Nell'era dell'interconnessione è sempre più difficile mettere al sicuro dati e informazioni. La trasformazione del modo di comunicare ha posto l'attenzione sulla necessità di proteggere adeguatamente i flussi di dati e i sistemi interconnessi. Al crescere della complessità delle architetture informatiche cresce da pari passo la complessità nel controllo manageriale sulle informazioni, sulle persone e sui mezzi predisposti per il loro trattamento. Le aziende sono esposte a gravi rischi spesso ignorati. Il corso vuole fornire agli studenti una panoramica sul contesto operativo della cyber security e sulla normativa Europea e Italiana relativa alla sicurezza dei dati e delle informazioni, fornendo gli strumenti necessari per comprendere il processo di governo della sicurezza e compliance aziendale alla normativa.

Gli obiettivi del corso sono di fornire agli studenti un approccio pratico e concreto al processo di governo e compliance all'IT security partendo dai concetti di sicurezza dei dati e delle informazioni attraverso una lettura completa e critica delle normative in tema di sicurezza dei dati e del loro trattamento.

Nell'ultima lezione del corso gli studenti parteciperanno all'analisi di un caso pratico di gestione di un incidente di sicurezza all'interno dell'azienda.

Alla fine del corso, i partecipanti saranno in grado di:

- Comprendere quali sono le principali minacce informatiche
- Comprendere come è possibile mitigare i rischi di un attacco informatico
- Comprendere le interdipendenze internazionali delle attività cyber
- Comprendere quali risorse aziendali sono necessarie nel processo di innalzamento del livello di sicurezza informatica
- Comprendere l'importanza della computer forensics per conservare le tracce di un incidente informatico (Forensics Readiness)

## Destinatari

Il corso è aperto a tutti gli studenti Bocconi. In particolare si rivolge a tutti coloro che sono interessati a comprendere il contesto giuridico e tecnologico e l'approccio in materia di compliance aziendale, sia dal punto di vista normativo che da quello

tecnologico. Per la natura degli argomenti trattati, è particolarmente indicato per gli studenti del CLMG e dei Corsi di Laurea Magistrale, in particolare del CLELI.

## Prerequisiti

Nessuno. Si consiglia tuttavia di aver superato un esame di informatica come Computer science o Informatica per giurisprudenza, o di possedere le competenze equivalenti.

## Modalità didattica

Sarà possibile partecipare al corso esclusivamente in maniera presenziale.

## Durata

10 ore

## Calendario

Lezione	Data	Ora	Aula
1	gio 23/03/2023	18.15 - 19.45	N18 (Velodromo)
2	mar 28/03/2023	18.15 - 19.45	N35 (Velodromo)
3	gio 30/03/2023	18.15 - 19.45	N18 (Velodromo)
4	mar 04/04/2023	18.15 - 19.45	N35 (Velodromo)
5	mer 05/04/2023	18.15 - 19.45	N35 (Velodromo)

## Programma delle lezioni

Lezione	Argomenti
1	<p><b>La sicurezza informatica</b></p> <ul style="list-style-type: none"> <li>- Definizioni (sicurezza dei dati e sicurezza delle informazioni)</li> <li>- Cyber security come gestione del rischio</li> <li>- I tipi di rischio: intrusion, furto di identità, interruzione di servizio</li> <li>- Le tecniche: phishing, intrusion, DDoS ecc.</li> <li>- I principali framework di riferimento per la Cyber security</li> </ul>

Lezione	Argomenti
<b>2</b>	<b>La sicurezza in azienda</b> <ul style="list-style-type: none"> <li>- Compliance aziendale</li> <li>- La normativa europea (ENISA, Direttive NIS)</li> <li>- Information warfare (la guerra delle informazioni)</li> <li>- Il GDPR</li> <li>- Policy e procedure</li> <li>- La gestione dell'incident (data breach)</li> <li>- Esempi pratici: le CEO Fraud</li> </ul>
<b>3</b>	<b>Il rischio cyber: difesa della superficie d'attacco</b> <ul style="list-style-type: none"> <li>- Mitigazione del rischio: approccio e misura</li> <li>- Misure Tecniche: <ul style="list-style-type: none"> <li>o perimetrale, interna, preventiva, reattiva</li> <li>o monitoraggio</li> </ul> </li> <li>- Sistemi di rilevazione degli incidenti di sicurezza e importanza del monitoraggio: SIEM, IoA e IoC, sistemi antifrode, VA ecc.</li> <li>- Velocità di ripristino vs. necessità di investigazione</li> <li>- Incident responding: identificazione del perimetro di intervento</li> <li>- Anonimizzazione e tracciabilità</li> </ul>
<b>4</b>	<b>Attacchi e prevenzioni</b> <ul style="list-style-type: none"> <li>- Misure Organizzative: <ul style="list-style-type: none"> <li>o Il fattore umano: Training, consapevolezza</li> <li>o I ruoli aziendali coinvolti: DPO, CISO, CRO</li> </ul> </li> <li>- Identificazione del problema, intervento, ripristino, notifica del breach</li> <li>- Unità di crisi multifunzionale</li> <li>- acquisizione forense delle evidenze, ripristino dei sistemi</li> <li>- Digital Forensics: investigazione con valore probatorio delle risultanze</li> <li>- Riferimenti normativi</li> <li>- La Forensic Readiness</li> </ul>
<b>5</b>	<b>Analisi di un caso pratico</b> <ul style="list-style-type: none"> <li>- Partendo da casi di cyber attacchi realmente accaduti, verrà analizzata la gestione della cyber crisis sotto il profilo tecnico, legale ed organizzativo.</li> <li>- Attività di debriefing del caso e analisi delle possibili soluzioni</li> </ul>

## Bibliografia suggerita

Materiali prodotti dai docenti

## Posti disponibili

Questa attività è a numero chiuso quindi l'iscrizione non sarà possibile oltre **110 posti** o dopo la chiusura del periodo di iscrizione.