

PROPOSTA DI ISTITUZIONE MASTER

A.A. 2026/2027

NUOVA PROPOSTA

DENOMINAZIONE DEL MASTER	Cybersecurity e Compliance Aziendale Integrata
DENOMINAZIONE IN INGLESE	<i>Cybersecurity and Integrated Corporate Compliance</i>
LIVELLO	II
ANNUALITÀ	annuale
DIPARTIMENTO DI AFFERENZA	Dipartimento di Ingegneria dell'Informazione
SEDE/I DI SVOLGIMENTO DELL'ATTIVITÀ DIDATTICA	Università degli Studi di Brescia
SEDE/I DI SVOLGIMENTO DEI TIROCINI	Università degli Studi di Brescia e in enti esterni con i quali saranno previste specifiche convenzioni
MASTER INTERATENEEO	

DIRETTORE/DIRETTRICE DEL MASTER:	Prof. Federico Cerutti
CONSIGLIO DIRETTIVO DEL MASTER	Prof. Federico Cerutti (Professore Ordinario, UniBS) Prof. Francesco Gringoli (Professore Ordinario, UniBS) Dott. Antonio Fiorentino (Ispettore della Polizia di Stato presso il Nucleo Operativo Centrale di Sicurezza - Sezione Operativa Sicurezza Cibernetica di Brescia) Prof. Matteo Frau (Professore Ordinario, UniBS) Prof. Giorgio Pedrazzi (Ricercatore Universitario, UniBS) Prof.ssa Francesca Romanin Jacur (Professoressa Associata, UniBS)
REFERENTE AMMINISTRATIVO/A	Dott. Vincenzo Canino vincenzo.canino@unibs.it

PROPOSTA DI ISTITUZIONE MASTER

DURATA	Il master ha durata di 1500 ore, di cui: - ore dedicate all'attività didattica frontale (lezioni): 300 ore (47 CFU) - ore dedicate allo stage aziendale (tirocinio): 250 ore (10 CFU), comprensive delle ore svolte presso l'organizzazione ospitante e delle attività funzionali e propedeutiche allo svolgimento dello stage stesso, quali, a titolo esemplificativo, l'analisi di normative tecniche, standard e framework di riferimento applicabili allo specifico contesto operativo e settoriale dell'azienda ospitante. In considerazione della natura evolutiva, interdisciplinare e fortemente contestuale delle tematiche di cybersecurity e di compliance aziendale integrata, nonché della pluralità di standard, linee guida e normative di riferimento (nazionali e internazionali) applicabili ai diversi settori, le modalità di svolgimento del tirocinio richiedono una definizione flessibile e adattabile ai diversi contesti. La distribuzione delle ore tra attività svolte in presenza presso l'azienda e attività preparatorie e di supporto direttamente connesse al progetto di stage sarà definita di volta in volta. Anche gli obiettivi formativi specifici saranno stabiliti caso per caso nell'ambito delle convenzioni con le aziende e dei relativi progetti formativi, al fine di garantire la coerenza con le esigenze formative del Master e con i contesti applicativi di riferimento. In tale quadro si individuano tre tipologie principali di tirocinio: una tipologia a bassa incidenza di preparazione individuale, fino a un massimo del 25% delle ore, riferita a contesti aziendali privi di specifiche peculiarità di dominio, nei quali lo/la studente, avendo già affrontato nel percorso formativo gli aspetti fondamentali, può inserirsi direttamente a supporto delle funzioni di cybersecurity e compliance, tipicamente in affiancamento al CISO (Chief Information Security Officer); una tipologia intermedia, con una quota di preparazione individuale fino a circa il 50% delle ore, relativa ad aziende con processi, tecnologie o vincoli regolatori specifici ma non altamente specialistici, che richiedono un adattamento mirato delle competenze acquisite al contesto operativo; e una tipologia ad alta incidenza di preparazione individuale, fino a un massimo del 75% delle ore, propria di settori fortemente specializzati, quali ad esempio l'automotive o il biomedicale, nei quali è necessaria un'approfondita comprensione preventiva del dominio, dei relativi standard tecnici e del quadro normativo settoriale prima dell'inserimento operativo in azienda. - ore dedicate allo studio individuale: 875 ore - preparazione tesi: 75 ore (3 CFU) Il master avrà inizio a ottobre 2026 e terminerà a ottobre 2027
CREDITI FORMATIVI UNIVERSITARI	60 CFU
ACCREDITAMENTI (se previsti)	Non previsti
QUOTA DI ISCRIZIONE	€ 7.296,00 (quota di Iscrizione di € 7.280,00 + € 16,00 di bollo)
UDITORI/UDITRICI (se previsti/e)	Limitatamente ai/lle dipendenti della Polizia Postale e solo nel caso questa fornisca la lettera di supporto entro il 31 marzo 2026, potrà essere prevista la partecipazione, in qualità di Uditori/rici, ad uno solo dei 5 insegnamenti previsti nel Piano Didattico ed unicamente da remoto.
NUMERO MINIMO E MASSIMO DI ISCRITTI/E	Minimo: 19 Massimo: 25 <i>Qualora non venga raggiunto il numero minimo, il corso non verrà attivato</i>

PROPOSTA DI ISTITUZIONE MASTER

MODALITÀ EROGAZIONE DIDATTICA	Mista (presenza e teledidattica in modalità sincrona).
LINGUA DI EROGAZIONE DELLA DIDATTICA	Italiano
PARTECIPAZIONE A SINGOLE LEZIONI/MODULI (se prevista)	Non prevista
FINALITÀ	La finalità del Master di secondo livello in Cybersecurity e Compliance Aziendale Integrata è formare figure di middle-management in grado di comprendere e governare in modo coordinato le dimensioni tecnologiche, giuridiche e organizzative della sicurezza dell'informazione. Il percorso mira a sviluppare profili capaci di dialogare sia con il top management sia con le funzioni tecniche, contribuendo alla definizione delle strategie di sicurezza, alla gestione del rischio digitale e all'allineamento continuo con il quadro normativo e regolatorio, in una prospettiva che può evolvere verso il ruolo di CISO.
OBIETTIVI FORMATIVI	Gli obiettivi formativi riguardano l'acquisizione di conoscenze avanzate in ingegneria dell'informazione, giurisprudenza della sicurezza, sicurezza delle reti, sicurezza dei sistemi di elaborazione tradizionali e sicurezza dei sistemi di intelligenza artificiale, con attenzione specifica alla compliance aziendale integrata. Il master intende sviluppare competenze operative in ambiti quali crittografia, digital forensics, incident management, cyber threat intelligence, gestione del rischio e delle identità digitali, oltre a capacità di analisi dei modelli organizzativi, delle responsabilità legali e dei profili etici. Il tirocinio formativo e la tesi finale consentono di consolidare tali competenze su casi reali e progetti applicati.
SBOCCHI PROFESSIONALI	Gli sbocchi professionali includono ruoli di responsabilità intermedia nelle funzioni di sicurezza informatica, IT, risk management, compliance, audit interno e nelle strutture dedicate alla governance dei sistemi informativi, tanto in organizzazioni private quanto in enti pubblici. I/le diplomati/e potranno operare come cybersecurity e compliance manager, referenti o coordinatori/rici per la sicurezza delle informazioni, figure di supporto alla funzione CISO o a strutture di SOC (Security Operation Centre) e system integration, nonché come consulenti in progetti di adeguamento normativo e di gestione integrata dei rischi tecnologici e organizzativi.
OBBLIGO DI FREQUENZA	Frequenza obbligatoria minima: 75% del monte ore complessivo.
PROVE D'ESAME E TESI FINALE	A metà e alla fine delle lezioni frontali, verranno somministrate prove d'esame con domande a scelta multipla per i diversi ambiti disciplinari. Al termine del corso, i/le candidati/e presenteranno una tesi finale.
REQUISITI PER L'ACCESSO	L'iscrizione al corso per l'acquisizione del titolo di Master è riservata ai/le titolari di Laurea specialistica ai sensi del D.M. 509/1999; magistrale ai sensi D.M. 270/2004; laurea a ciclo unico di Vecchio Ordinamento (antecedente D.M. 509/1999). I titoli devono risultare conseguiti entro e non oltre la data di scadenza del Bando. I/le candidati/e in possesso di titolo di studio straniero non preventivamente dichiarato equipollente da parte di una autorità accademica italiana potranno chiedere al Consiglio Direttivo del Master il riconoscimento del titolo ai soli limitati fini dell'iscrizione al Master.

PROPOSTA DI ISTITUZIONE MASTER

CRITERI E MODALITÀ DI SELEZIONE	Qualora il numero delle domande di iscrizione superi il numero massimo di partecipanti che possono essere ammessi/e al Master, l'ammissione avverrà secondo l'ordine cronologico di presentazione delle iscrizioni.
PREMI / BORSE (se previsti)	Non previsto
ESONERO PAGAMENTO PER INVALIDITÀ	Non previsto
PARTNER ESTERNI	Le seguenti aziende o istituzioni hanno firmato una lettera di supporto alla proposta di istituzione di tale master, che vengono allegate alla presente documentazione: • Camera di Commercio di Brescia • Confindustria Brescia • ONIF - Osservatorio Nazionale per l'Informatica Forense • CLUSIT - Associazione Italiana per la Sicurezza Informatica • Vexo S.r.l. • Nemesi Italia S.r.l. • Errecom S.p.A. • Cavagna Group / Parteca S.p.A. • Ferapli Group • CINI Cybersecurity National Laboratory • Camera Civile di Brescia • Ordine degli Avvocati della Provincia di Brescia • A2A • Ordine degli Ingegneri della Provincia di Brescia • PersonalData Siamo inoltre in contatto con le seguenti aziende/istituzioni potenzialmente interessate a collaborare al Master, le quali dovranno fornire la lettera di supporto entro il 31 marzo 2026, per poter rientrare ufficialmente tra i partner del Master: • Fondazione A.I.B. • ISFOR Brescia • Confapi Brescia • Unimatica Brescia • Camozzi • ACN • Polizia Postale • Fondazione Bresciana per gli Studi Economico-Giuridici • InnexHub • Guber • ATM • YARIX • Appleby
NOTE	Il corpo docente e il direttivo del master al momento non riflette un equilibrio di genere, con una predominanza di docenti di sesso maschile — intorno all'84%. Questo rispecchia una tendenza osservata nel settore della cybersecurity, dove le donne costituiscono in media una quota relativamente bassa della forza lavoro specializzata (tra il 15 e il 20 per cento a livello globale secondo studi recenti, ad esempio https://www.isc2.org/Insights/2024/08/Cybersecurity-Gender-Imbalance-in-the-Spotlight). Il consiglio direttivo è consapevole di questa disparità e sensibile alle tematiche di inclusione di genere, tanto che il master include un modulo dedicato alle questioni di genere nella cybersecurity per promuovere consapevolezza e competenze critiche su questi aspetti. Si richiede, in accordo con la previsione dell'art. 18, comma 8, del "Regolamento

PROPOSTA DI ISTITUZIONE MASTER

per l'attivazione, l'organizzazione e la gestione di Master Universitari di I e II livello e Corsi di Perfezionamento", che il Consiglio di Amministrazione disponga che l'utile generato dal Master venga destinato alle attività di ricerca del proponente e ad eventuali edizioni successive del Master stesso

DOCUMENTI ALLEGATI ALLA PROPOSTA

X PIANO DIDATTICO

X PIANO FINANZIARIO E PIANO COAN

X CALENDARIO/PROGRAMMA

X LETTERE DI INTENTI

X EVENTUALE ALTRA DOCUMENTAZIONE:

- Modulo assenza conflitto di interessi
- Prospetto costi docenza

ATTENZIONE:

la proposta di attivazione dovrà essere deliberata entro il 31 marzo dell'anno accademico antecedente a quello di svolgimento, per i Master la cui attivazione è prevista nel primo semestre, entro il 30 settembre dell'anno accademico precedente a quello di svolgimento, per i Master la cui attivazione è prevista nel secondo semestre.

Il Direttore del Master
Prof. Federico Cerutti

Firmato digitalmente da Federico Cerutti
Data: 30.03.2026 11:34:17 CEST
Organizzazione: UNIVERSITA' DEGLI STUDI DI BRESCIA/01773710171