Regolamento Corso di formazione online «Cybersecurity: dai Fondamenti alle Tecniche Avanzate di Sicurezza- Edizione 2026»

Roma, luglio 2026

1. Premessa

Nell'ambito del progetto "Cyber Sapere", promosso dal Ministero dell'Università e della Ricerca (MUR) tramite la Direzione Generale del Personale, del Bilancio, dei Servizi Strumentali e della Comunicazione, sarà organizzato, dal 20 luglio al 9 ottobre 2026, il corso di formazione online "Cybersecurity: dai fondamenti alle tecniche avanzate di sicurezza – Edizione 2026", finalizzato a rafforzare la consapevolezza e le competenze in materia di cybersicurezza.

Il presente documento ha lo scopo di fornire ai partecipanti il regolamento del corso di formazione online, illustrandone le principali caratteristiche e le linee guida necessarie a garantire una fruizione corretta, efficace e consapevole delle attività formative.

2. Modalità di accesso degli utenti

Il corso di formazione online si svolge in modalità asincrona sulla piattaforma Moodle ed è rivolto al personale docente e tecnico-amministrativo degli Atenei e delle Istituzioni di Alta Formazione Artistica, Musicale e Coreutica (AFAM).

L'iscrizione del personale degli IFS è stata effettuata dal Referente della formazione del rispettivo Istituto di appartenenza che, in fase di compilazione dell'apposito form di registrazione, ha provveduto a inserire, per ciascun partecipante, i dati identificativi richiesti, nello specifico: nome, cognome, indirizzo e-mail istituzionale e codice fiscale.

Nell'ambito della presente iniziativa formativa, è stata inoltre condivisa con tutti i partecipanti l'informativa sul trattamento dei dati personali, resa ai sensi dell'art. 13 del GDPR.

L'accesso alla piattaforma Moodle avviene tramite SPID.

3. Accessibilità dei corsi di formazione

La piattaforma Moodle è dotata di strumenti idonei a garantire l'accessibilità e la piena fruizione dei contenuti formativi da parte di tutti gli utenti. I materiali didattici e le informazioni rese disponibili nell'ambito del corso sono progettati nel rispetto dei principi di inclusività, accessibilità e pari opportunità, al fine di consentirne l'utilizzo da parte del più ampio numero possibile di destinatari.

Le videolezioni sono corredate da materiale didattico in formato PDF e da trascrizioni testuali dei principali contenuti grafici e informativi presenti nelle singole lezioni, compatibili con i software di lettura dello schermo (screen reader).

I contenuti multimediali sono inoltre dotati di sottotitoli sincronizzati, che consentono la trascrizione testuale dell'audio e favoriscono una più agevole comprensione e fruizione dei contenuti formativi.

4. Fruizione dei contenuti

Il corso online «Cybersecurity: dai Fondamenti alle Tecniche Avanzate di Sicurezza – Edizione 2026» è un'iniziativa formativa dedicata alla sicurezza informatica, finalizzata a supportare i discenti nel riconoscimento e nella prevenzione dei principali rischi digitali.

Il corso si articola in due moduli e prevede una durata complessiva di **28 ore**. Tutte le lezioni saranno rese disponibili contemporaneamente, al fine di consentire ai partecipanti di organizzare autonomamente il proprio percorso di apprendimento, gestendo tempi e modalità di fruizione secondo le proprie esigenze.

Il superamento del quiz previsto al termine di ciascuna lezione costituisce requisito indispensabile per l'accesso alla lezione successiva, garantendo in tal modo una progressione strutturata e coerente dell'apprendimento lungo l'intero percorso formativo.

Di seguito si riporta il dettaglio dei moduli e delle relative lezioni:

ID MODULO	TITOLO LEZIONI
Modulo 1: Introduzione alla Cyber Security	Introduzione ai Principi Fondamentali di Cyber Security – Parte 1
	Introduzione ai Principi Fondamentali di Cyber Security – Parte 2
	Evoluzione delle minacce e tendenze nella Cyber Security – Parte 1
	Evoluzione delle minacce e tendenze nella Cyber Security – Parte 2
	Fonti di Threat Intelligence: OSINT, Deep e Dark Web – Parte 1
	Fonti di Threat Intelligence: OSINT, Deep e Dark Web – Parte 2
	Best Practices nella Risposta alle Minacce Informatiche – Parte 1
	Best Practices nella Risposta alle Minacce Informatiche – Parte 2
Modulo 2: Cyber Security e Data Protection	Direttiva NIS 2: obblighi, responsabilità e opportunità – Parte 1

	Direttiva NIS 2: obblighi, responsabilità e opportunità – Parte 2
	Il ruolo del Garante della Privacy e dell'Agenzia per la Cybersicurezza Nazionale (ACN) - Parte 1
	Il ruolo del Garante della Privacy e dell'Agenzia per la Cybersicurezza Nazionale (ACN) - Parte 2
	Framework e Standard di Cyber security – Parte 1
	Framework e Standard di Cyber security – Parte 2
	Misure di sicurezza per i dati personali & incidenti di sicurezza, Data Breach e Data Leak – Parte 1
	Misure di sicurezza per i dati personali & incidenti di sicurezza, Data Breach e Data Leak – Parte 2

4.1. Modulo 1: Introduzione alla Cyber Security

Il primo modulo del corso è composto dalle seguenti lezioni:

1. **Introduzione ai Principi Fondamentali di Cyber Security - Parte 1:** nella lezione viene fornita una panoramica sull'importanza dell'informazione come asset strategico per Pubbliche Amministrazioni e organizzazioni private, a supporto di decisioni e processi. Dati, informazioni e conoscenza costituiscono una catena di valore che deve essere protetta secondo i principi di riservatezza, integrità e disponibilità (RID). Vengono analizzate le principali tendenze emergenti, come gli attacchi ransomware, e l'evoluzione tecnologica del panorama delle minacce che influenza le scelte strategiche delle organizzazioni e delle società per mitigare i principali rischi cyber.
2. **Introduzione ai Principi Fondamentali di Cyber Security - Parte 2:** nella lezione è raccontata l'evoluzione della figura degli hacker, oggi composta da attori eterogenei che spaziano da professionisti della sicurezza a gruppi criminali organizzati e collettivi sponsorizzati da stati. Viene illustrata la classificazione white hat, grey hat e black hat e il ruolo del surface, deep e dark web nella diffusione e nel commercio illecito dei dati. Si evidenzia come la Cyber Security coinvolga tutta l'organizzazione attraverso buone pratiche, strumenti di monitoraggio (SOC e NOC) e responsabilità distribuite tra

governance e personale operativo. Sono inoltre richiamati i principali riferimenti normativi e framework internazionali (NIS/NIS2, ACN, ISO, NIST, GDPR) e i ruoli di strutture come CSIRT e CVCN nella protezione dei dati personali e delle infrastrutture critiche.

3. **Evoluzione delle minacce e tendenze nella Cyber Security - Parte 1:** nella lezione viene presentata una panoramica delle principali tipologie di attacco cyber, con un inquadramento del fenomeno e della sua recente evoluzione in Italia. Si introducono le categorie di minaccia, le finalità degli attaccanti, l'aumento degli incidenti e le tecniche e i target più comuni. Vengono poi approfonditi il malware, con le principali famiglie e caratteristiche di pericolosità, il ransomware, illustrandone funzionamento, impatti, motivi per cui non pagare il riscatto e principali contromisure, e infine il social engineering, analizzando vettori di attacco, forme di phishing e best practices di prevenzione in ambito digitale e lavorativo.
4. **Evoluzione delle minacce e tendenze nella Cyber Security - Parte 2**: nella lezione vengono analizzate le ulteriori minacce, con focus sugli attacchi alle password, sui DDoS e sugli attacchi alla supply chain. Si descrivono le principali tecniche di compromissione delle credenziali e l'importanza della loro robustezza, il funzionamento e la mitigazione degli attacchi DDoS a tutela della continuità dei servizi, le contromisure tecniche come firewall, IDS/IPS e monitoraggio del traffico, e infine i supply chain attack, evidenziando modalità di propagazione e strategie di difesa basate su valutazione dei fornitori, sicurezza contrattuale e piani di risposta agli incidenti.
5. **Fonti di Threat Intelligence: OSINT, Deep e Dark Web - Parte 1:** la lezione propone una visione d'insieme dell'intelligence nel contesto della cybersicurezza, partendo dai concetti introduttivi essenziali. Vengono esaminate le principali categorie di intelligence, mettendone in evidenza le caratteristiche distintive e gli ambiti di utilizzo, per poi approfondire i principi fondamentali della Threat Intelligence, intesa come strumento centrale per l'individuazione e la gestione delle minacce informatiche.
6. **Fonti di Threat Intelligence: OSINT, Deep e Dark Web - Parte 2:** nel corso della lezione vengono approfonditi i principi della Threat Intelligence, con un'attenzione specifica alla metodologia OSINT (Open Source Intelligence), analizzata come processo strutturato di raccolta, analisi e correlazione di informazioni provenienti da fonti aperte attraverso l'utilizzo di specifici tool di intelligence, tra cui motori di ricerca avanzati, piattaforme di data aggregation e strumenti dedicati all'analisi delle reti e delle superfici esposte. L'approfondimento include inoltre lo studio del Deep Web e del Dark Web, esaminandone le differenze tecniche e operative, le modalità di accesso e monitoraggio tramite strumenti specializzati, nonché le implicazioni strategiche che tali ambienti presentano per l'identificazione tempestiva delle minacce e per le attività di sicurezza informatica.
7. **Best Practices nella Risposta alle Minacce Informatiche - Parte 1:** nel corso della lezione viene proposta un'analisi articolata del quadro complessivo della sicurezza informatica, con particolare attenzione agli organismi, alle strutture e agli strumenti

deputati alla prevenzione, al monitoraggio e alla gestione degli eventi di sicurezza. L'obiettivo è fornire una visione sistemica delle funzioni di protezione dei sistemi informativi all'interno delle organizzazioni moderne. In questo contesto, vengono introdotti e approfonditi i concetti chiave di Security Operations Center (SOC) e Computer Security Incident Response Team (CSIRT), descrivendone l'organizzazione, le responsabilità operative e il ruolo strategico nel ciclo di vita della sicurezza.

8. **Best Practices nella Risposta alle Minacce Informatiche - Parte 2:** nel corso della lezione viene approfondito il modello della Cyber Kill Chain, utilizzato come chiave interpretativa per analizzare in modo strutturato le diverse fasi che caratterizzano un attacco informatico, dalla ricognizione iniziale fino al raggiungimento degli obiettivi dell'attaccante. L'analisi teorica è affiancata da un caso di studio pratico, basato su un incidente reale, che permette di applicare i concetti illustrati e di osservare concretamente l'evoluzione di un attacco e le relative strategie di risposta. La lezione si conclude con un approfondimento dedicato alla Digital Forensics, presentata come disciplina fondamentale per l'analisi post-incidente e il supporto alle attività investigative.

4.2. Modulo 2: Cyber Security e Data Protection

Il secondo modulo del corso è composto dalle seguenti lezioni:

1. **Direttiva NIS2: obblighi, responsabilità e opportunità – Parte 1.** La lezione propone una panoramica strutturata della Direttiva NIS2, con particolare attenzione alle modalità di recepimento nell'ordinamento italiano. L'analisi ripercorre il passaggio dalla Direttiva NIS alla NIS2, evidenziandone l'evoluzione normativa, il rafforzamento degli obiettivi e la nuova impostazione sistemica. Viene inoltre approfondita la Strategia Nazionale per la Cybersicurezza, evidenziandone il ruolo nel quadro complessivo di tutela degli asset digitali. La lezione si sofferma infine sui meccanismi di cooperazione a livello europeo, finalizzati alla gestione coordinata delle crisi cibernetiche e al rafforzamento della fiducia reciproca e del coordinamento operativo tra le autorità competenti.
2. **Direttiva NIS2: obblighi, responsabilità e opportunità – Parte 2.** La lezione approfondisce in modo organico la struttura della Direttiva e i criteri che ne regolano l'applicazione, con particolare attenzione alla gestione dei rischi di sicurezza informatica. Vengono inoltre analizzati i profili di giurisdizione e il funzionamento dei meccanismi di cooperazione tra gli Stati membri, con specifico riferimento agli accordi di condivisione delle informazioni. Il percorso prosegue con l'analisi dei sistemi di vigilanza e di esecuzione, dell'impianto sanzionatorio e degli atti delegati e di esecuzione adottati dalla Commissione europea, per concludersi con l'inquadramento dei ruoli e delle responsabilità delle principali figure professionali individuate dall'ENISA, fondamentali per il conseguimento di un adeguato livello di resilienza cibernetica.

3. **Il ruolo del Garante della Privacy e dell'Agenzia per la Cybersicurezza Nazionale (ACN) – Parte 1.** La lezione illustra le principali istituzioni e autorità europee coinvolte nella cybersicurezza e nella protezione dei dati personali, evidenziandone il ruolo di supporto agli Stati membri nella definizione di politiche digitali comuni, nella gestione dei rischi cyber e nella tutela dei diritti fondamentali. Segue un approfondimento dedicato all'ENISA, con focus sulle attività di supporto tecnico e operativo in materia di cybersicurezza, sullo sviluppo di linee guida, framework ed esercitazioni cyber, nonché sul rafforzamento della resilienza delle infrastrutture critiche. Viene inoltre analizzato il ruolo dell'European Data Protection Board (EDPB), con riferimento alle funzioni di coordinamento tra le autorità nazionali, all'applicazione uniforme del GDPR e all'adozione di pareri, raccomandazioni e decisioni vincolanti nei casi transfrontalieri. La lezione si conclude con un approfondimento dedicato a Europol e alle attività di contrasto alla criminalità informatica, di supporto alle indagini transnazionali e di cooperazione informativa tra le forze di polizia, anche attraverso strutture specializzate quali l'EC3.
4. **Il ruolo del Garante della Privacy e dell'Agenzia per la Cybersicurezza Nazionale (ACN) – Parte 2.** Nel corso della lezione viene analizzato il ruolo dell'Agenzia per la Cybersicurezza Nazionale (ACN), approfondendone le funzioni di coordinamento delle politiche di sicurezza cyber, di protezione delle infrastrutture critiche e di supporto alle Pubbliche Amministrazioni e agli operatori di servizi essenziali. Successivamente viene esaminata l'attività del Garante per la protezione dei dati personali, con particolare attenzione alla vigilanza sull'applicazione del GDPR e alla tutela dei diritti degli interessati. La lezione approfondisce infine il ruolo della Polizia Postale nelle attività di prevenzione e contrasto della criminalità informatica, nel supporto alle indagini e nella cooperazione operativa.
5. **Framework e Standard di Cyber Security – Parte 1.** La lezione introduce il concetto di framework e standard nell'ambito della cybersicurezza, illustrandone le principali caratteristiche e le differenze sostanziali. Viene successivamente approfondito il ruolo del National Institute of Standards and Technology (NIST) nel panorama internazionale della sicurezza informatica, con particolare attenzione al Cyber Security Framework (CSF). Ne vengono analizzate la struttura, i livelli di implementazione (tiers), i profili e le sei funzioni fondamentali — Govern, Identify, Protect, Detect, Respond e Recover — esaminate nei rispettivi obiettivi e nelle implicazioni operative. La lezione si conclude con una panoramica applicativa del CSF quale strumento di security assessment, evidenziandone l'utilizzo per supportare un percorso strutturato di miglioramento continuo della sicurezza informatica all'interno dell'Amministrazione.
6. **Framework e Standard di Cyber Security – Parte 2.** La lezione fornisce una panoramica delle principali caratteristiche degli standard di cyber security, con particolare focus sulla famiglia ISO/IEC 27000. Ne vengono illustrate la struttura complessiva, la logica di composizione dei diversi standard e i relativi ambiti di applicazione. Viene inoltre introdotto il concetto di standard certificabile e descritto il

relativo processo di certificazione. Il percorso prosegue con l'analisi del ciclo Plan-Do-Check-Act (PDCA) quale modello di riferimento per la conformità normativa e il miglioramento continuo, con la definizione del concetto di information security governance e con l'approfondimento della ISO/IEC 27001 quale standard di riferimento per la progettazione e il mantenimento di un sistema di gestione della sicurezza delle informazioni (ISMS). La lezione si conclude con la definizione di business continuity e con l'analisi della ISO 22301 quale standard di riferimento per la resilienza operativa e la continuità dei servizi critici.

7. **Misure di sicurezza per i dati personali e incidenti di sicurezza, data breach e data leak – Parte 1.** La lezione fornisce la definizione di incidente di sicurezza secondo i principali standard e le normative di riferimento, classificando gli eventi sulla base della loro natura e del grado di intenzionalità. Vengono quindi analizzate le principali tipologie di incidente e il relativo impatto, sia in termini di danno potenziale sia di danno effettivo, con riferimento al modello RID (Riservatezza, Integrità, Disponibilità). Il percorso prosegue con la distinzione tra data leak e data breach, illustrandone caratteristiche, implicazioni normative e operative, e con una panoramica delle principali cause degli incidenti di sicurezza, supportata da casi studio reali.
8. **Misure di sicurezza per i dati personali e incidenti di sicurezza, data breach e data leak – Parte 2.** La lezione, conforme alle Linee guida NIS sulla gestione degli incidenti di sicurezza informatica, offre una visione d'insieme dell'intero processo di incident management, approfondendone le singole fasi, le relative sottofasi e gli obiettivi da conseguire. Viene inoltre presentata una panoramica dei principali ruoli coinvolti nel processo di gestione degli incidenti, con particolare attenzione agli obblighi normativi di segnalazione verso le autorità nazionali competenti. La lezione si conclude con l'analisi degli errori più comuni da evitare nella predisposizione delle notifiche, al fine di garantire comunicazioni complete, accurate e conformi ai requisiti normativi, riducendo il rischio di segnalazioni incomplete o non corrette.

5. Repository documentale

La piattaforma Moodle mette a disposizione un repository documentale finalizzato a supportare il processo di apprendimento degli utenti, favorendo una fruizione flessibile dei contenuti e un apprendimento progressivo lungo l'intero percorso formativo.

I materiali didattici sono organizzati all'interno delle diverse sezioni del corso e risultano scaricabili dagli utenti, così da consentirne una consultazione agevole anche in modalità offline.

In particolare, la piattaforma rende disponibili differenti tipologie di contenuti, tra cui videolezioni, materiale didattico in formato PDF a supporto delle singole lezioni, trascrizioni

degli elementi grafici con finalità formative e test di valutazione intermedia previsti al termine di ciascuna sessione formativa.

6. Tracciamento delle attività degli utenti

La piattaforma Moodle registra automaticamente tutte le attività svolte dagli utenti, memorizzandole in appositi registri che raccolgono informazioni di dettaglio relative all'identità dell'utente, all'avvio e al completamento delle singole lezioni. Si specifica, inoltre, che tali informazioni vengono registrate e conservate per un arco temporale limitato, esclusivamente per le finalità di monitoraggio connesse all'iniziativa formativa.

7. Test di valutazione intermedia non valutativi

All'interno della piattaforma sono presenti quiz somministrati al termine di ciascuna lezione e utilizzati quali criteri di completamento delle relative attività formative. Tali test non hanno finalità strettamente valutative, ma costituiscono uno strumento di supporto volto a consentire ai partecipanti di verificare il livello di apprendimento e le competenze acquisite a seguito della fruizione delle singole sessioni formative.

Pur essendo possibile consultare in qualsiasi momento tutti i contenuti del corso, lo svolgimento dei test segue un percorso sequenziale: ciascun test può essere effettuato solo dopo aver completato il precedente. Ai fini del completamento del corso e del rilascio dell'attestato di partecipazione è necessario completare tutti i test intermedi previsti.

I quiz di valutazione intermedia sono composti da 10 domande a risposta multipla. Il superamento di ciascun quiz costituisce requisito obbligatorio per l'accesso alla videolezione successiva, garantendo in tal modo una fruizione progressiva, strutturata e coerente dell'intero percorso formativo.

8. Test finale di verifica delle competenze acquisite

Il test finale di verifica delle competenze acquisite sarà erogato direttamente tramite la piattaforma Moodle e sarà accessibile esclusivamente ai discenti che avranno completato l'intero percorso formativo, mediante la visualizzazione di tutte le lezioni disponibili e il superamento dei quiz previsti al termine di ciascuna sessione formativa. Il test finale resterà disponibile fino al 9 ottobre 2026.

Il test sarà composto da 24 domande a risposta multipla, relative alle principali tematiche affrontate nel corso e, ai fini del superamento, sarà necessario rispondere correttamente ad almeno 14 domande.

Il tempo a disposizione per il completamento del test sarà pari a 30 minuti e la prova potrà essere sostenuta una sola volta, senza possibilità di ripetizione.

La piattaforma Moodle provvederà automaticamente al calcolo del punteggio conseguito dall'utente, fornendo un riscontro immediato dell'esito della prova.

9. Attestato di partecipazione

Per ciascun discente che avrà superato con esito positivo il test finale di verifica delle competenze acquisite, al termine del corso sarà reso disponibile l'attestato di partecipazione, scaricabile dall'apposita sezione della piattaforma Moodle. L'attestato riporterà i dati identificativi del partecipante (nome e cognome), l'indicazione del superamento del test finale e il numero di ore formative riconosciute.

L'attestato potrà essere trasmesso dal discente al proprio Ente di appartenenza, che valuterà l'eventuale computabilità delle ore formative maturate nell'ambito del monte ore complessivo delle 40 ore annue obbligatorie previste dalla direttiva del Ministro per la Pubblica Amministrazione del 14 gennaio 2025, recante «Valorizzazione delle persone e produzione di valore pubblico attraverso la formazione. Principi, obiettivi e strumenti».

10. Assistenza agli utenti

Al fine di garantire un adeguato supporto durante la fruizione del corso di formazione online, è prevista la seguente tipologia di assistenza:

- **Supporto informativo**: per richieste di chiarimenti o informazioni inerenti ai contenuti e all'organizzazione del percorso formativo, sarà possibile inviare una comunicazione all'indirizzo e-mail: Cyber_Sapere@mur.gov.it.