ANNO ACCADEMICO 2026/2027

BANDO DI SELEZIONE PER BORSE DI STUDIO

Per la partecipazione al Corso di Alta Formazione

"CYBERSECURITY E GESTIONE DEL RISCHIO GLOBALE"

PREMESSA

La Scuola di Politiche Economiche e Sociali "Carlo Azeglio Ciampi" (SPES Academy) e **Cassa Depositi e Prestiti, co-titolari del corso di alta formazione "Cybersecurity e Gestione del Rischio Globale"**, uniscono competenze strategico-istituzionali e tecnico-operative per contribuire alla formazione del capitale umano nel settore della sicurezza cibernetica. In uno scenario segnato da profonde trasformazioni geopolitiche, digitali e tecnologiche, il percorso risponde all'esigenza di sviluppare competenze multidisciplinari e nuovi modelli di leadership, capaci di guidare le istituzioni e le imprese nella gestione del rischio.

La collaborazione si inserisce nella missione di SPES Academy di "formare persone, per riformare le istituzioni", ripensando i modelli educativi per una nuova idea di Scuola "Sistema Paese".

Nata nel 2013 con la finalità di contribuire a formare persone in grado di assumere decisioni consapevoli e coraggiose, SPES Academy si ispira all'esempio di Carlo Azeglio Ciampi, Presidente emerito della Repubblica italiana, e al suo costante invito a educare i giovani all'impegno civile e alla responsabilità. Per tale ragione, Egli affermava che «la Scuola è parte vitale della Nazione: è il vivaio dell'Italia del futuro».

Da questo monito trae ispirazione l'impegno a promuovere, a livello nazionale e transnazionale, un "patto delle competenze" che favorisca il dialogo tra mediatori e policy maker e metta in relazione le risorse umane delle istituzioni nazionali, della Pubblica Amministrazione, della grande industria e delle PMI, dei media e della società civile, del mondo accademico e della ricerca. L'obiettivo è sviluppare le competenze necessarie per interpretare il cambiamento e rafforzare la consapevolezza e la responsabilità su temi di rilevanza strategica per l'Italia e l'Europa.

LA SECONDA EDIZIONE: CONTINUITÀ E INNOVAZIONE DEL PERCORSO FORMATIVO

Sulla scorta del successo della prima edizione del corso "Cybersecurity & Fraud Management", co-organizzata per l'anno accademico 2025/2026, **SPES Academy e** Cassa Depositi e Prestiti proseguono il percorso congiunto con una **seconda edizione**, ampliata e rinnovata nei contenuti, dal titolo "**Cybersecurity e Gestione del Rischio Globale**".

La seconda edizione del corso si inserisce in un contesto geopolitico e tecnologico profondamente mutato rispetto all'anno precedente: l'accelerazione dell'intelligenza artificiale generativa, l'inasprimento delle tensioni nel cyberspazio a livello internazionale e la cc.dd. "guerra ibrida", l'entrata in vigore delle principali normative europee (NIS2, DORA, AI Act) e la crescente consapevolezza circa la carenza strutturale di capitale umano qualificato nel settore cyber rendono necessario un aggiornamento dei contenuti e un ampliamento del corpo docenti.

Il percorso integra i contributi complementari dei due co-titolari: **Cassa Depositi e Prestiti** assicura, attraverso il proprio team di sicurezza, il presidio tecnico-operativo e l'analisi di casi reali del settore; SPES Academy cura la cornice strategico-istituzionale, con particolare attenzione alla geopolitica del cyberspazio, alla sovranità digitale e alla cyber diplomacy, coinvolgendo, attraverso il proprio Alto Consiglio e la rete istituzionale, un corpo docente di profilo apicale.

La seconda edizione si arricchisce inoltre del contributo di nuovi docenti, che affiancano il corpo docente di Cassa Depositi e Prestiti e al suo team di Cybersicurezza. Al consolidato patrimonio di competenze tecnico-operative di CDP si affiancano ulteriori professionalità provenienti dalle istituzioni, dall'accademia, dal mondo delle imprese e dai settori specialistici della gestione del rischio e della compliance. L'ampliamento del corpo docente valorizza il confronto tra esperienze e prospettive diverse, rafforzando il carattere multidisciplinare del corso e il collegamento tra visione strategica, innovazione tecnologica e applicazione concreta.

UN PATTO DELLE COMPETENZE: VISIONE STRATEGICA E FORMAZIONE APPLICATA

Trasformare la conoscenza in capacità di azione: è questo l'obiettivo del percorso promosso da SPES Academy e Cassa Depositi e Prestiti. Gli indirizzi didattico-strategici, definiti dall'Alto Consiglio della SPES Academy, puntano a formare professionisti capaci di leggere scenari complessi, affrontare problemi concreti e guidare il cambiamento nelle amministrazioni e nelle imprese.

- La formazione unisce **visione strategica, competenze multidisciplinari e applicazione pratica**. Il confronto con top executive, policy maker ed esperti di settori diversi aiuta i partecipanti a sviluppare pensiero critico, problem solving e nuove capacità di leadership. Il lavoro in team e la redazione di un Policy Paper condiviso permettono di tradurre quanto appreso in analisi e proposte, rafforzando anche la capacità di comunicare in modo chiaro e mirato.
- Il "patto delle competenze" mette in relazione **istituzioni, imprese, università e ricerca**, favorendo lo scambio di esperienze, il trasferimento tecnologico e la cooperazione nazionale e internazionale. L'obiettivo è avvicinare formazione e mondo del lavoro, valorizzando talenti e professionalità diverse per rispondere alle sfide della digitalizzazione, dell'innovazione e della resilienza.

Il percorso promuove una leadership responsabile, fondata sul rispetto dei diritti, delle libertà fondamentali e dei valori democratici e sull'inclusione. Innovazione e sostenibilità ne orientano l'approccio, al servizio dei settori strategici e dell'interesse pubblico.

Art. 1 - OGGETTO DEL BANDO

La Scuola di Politiche Economiche e Sociali "Carlo Azeglio Ciampi", promossa dalla Fondazione AISES ETS con sede a Roma, in Via Flaminia n. 141, 00196, in collaborazione con Cassa Depositi e Prestiti, bandisce una selezione a numero chiuso per la partecipazione alla seconda edizione del corso di alta formazione intitolato: **"Cybersecurity e Gestione del Rischio Globale"**.

Il corso mira a fornire una cornice concettuale e operativa di eccellenza sulla governance del rischio cyber attraverso il trasferimento di competenze multidisciplinari per bilanciare innovazione, conformità legale e resilienza.

Art. 2 - OBIETTIVI FORMATIVI

Il corso è destinato a fornire una cornice concettuale e operativa di eccellenza sulla governance del rischio cyber. Attraverso l'analisi dei nuovi framework europei (NIS2, DORA, AI Act), il percorso intende formare figure professionali con competenze ibride, capaci di operare efficacemente nel punto di incontro tra strategia, tecnologia, regolamentazione e gestione operativa del rischio. Tenuto conto dell'esperienza maturata nella prima edizione, la seconda edizione prevede un ampliamento del corpo docenti, nuovi temi quali cyber insurance, guerra cognitiva e disinformazione, protezione della supply chain e delle PMI e workshop applicativi rinnovati.
Le novità della seconda edizione sono illustrate nel dettaglio all'Art. 5 del presente bando.

Art. 3 - DESTINATARI

Il corso si rivolge a profili che intendono acquisire o rafforzare competenze nel campo della cybersecurity con una visione strategica e multidisciplinare. La classe sarà composta in modo eterogeneo da:

- Professionisti della sicurezza informatica, della gestione del rischio e della compliance (CISO, Security Manager, Risk Manager, DPO);
- Funzionari pubblici, dirigenti e operatori della Pubblica Amministrazione, delle Forze Armate e delle Forze dell'ordine;
- Manager e quadri del settore privato, in particolare dei comparti finanziario, energetico, delle telecomunicazioni e delle infrastrutture critiche;
- Avvocati, consulenti ed esperti di regolamentazione e digital policy;
- Laureati, dottorandi e ricercatori interessati ad approfondire le dinamiche della sicurezza cibernetica e della governance digitale.

Art. 4 - ORGANIZZAZIONE DEL CORSO

La seconda edizione del corso si inserisce in un contesto geopolitico e tecnologico profondamente mutato: l'accelerazione dell'intelligenza artificiale generativa, l'inasprimento delle tensioni nel cyberspazio a livello internazionale, l'entrata in vigore delle principali normative europee (NIS2, DORA, AI Act) e la crescente consapevolezza circa la carenza strutturale di capitale umano qualificato nel settore cyber rendono necessario un aggiornamento dei contenuti e un ampliamento del corpo docenti.

Il corso avrà luogo a Roma e si svolgerà in collaborazione con Cassa Depositi e Prestiti e con i partner istituzionali e aziendali coinvolti. Si articolerà secondo un modulo formativo in formato ibrido che prevede lo svolgimento delle lezioni con obbligo di frequenza da parte degli studenti, sia in presenza sia da remoto, sulla piattaforma e-learning.

Il percorso formativo avrà una durata complessiva di **(3) tre mesi** e sarà articolato in **4 moduli tematici**, con lezioni a cadenza settimanale di durata variabile di due o di quattro ore ciascuna secondo un calendario che coinvolgerà esponenti di governo e di istituzioni, esperti, leader aziendali, professionisti e accademici altamente specializzati e con profilo internazionale.

Il percorso adotta un modello didattico **ibrido,** strutturato per garantire la massima flessibilità e compatibilità con l'attività lavorativa:

- **Lezioni in modalità e-learning:** La quota prevalente delle lezioni teoriche si svolgerà online sulla piattaforma didattica della Scuola;
- **Sessioni in presenza**: Saranno previsti *high-level seminar*, *lectio magistralis* ed eventi di networking a Roma, ospitati presso spazi appositamente individuati in sedi istituzionali, aziende partner, università e centri di ricerca.

Ad ogni studente sarà rilasciato un *Diploma di Alta Formazione* attestante la partecipazione alla Scuola di Politiche Economiche e Sociali "Carlo Azeglio Ciampi", che sarà condizionato alla frequenza rilevata di una quota minima di ore obbligatorie, corrispondente al 70% delle ore totali.

Tavoli di lavoro e Policy Brief: Parte integrante e forte valore aggiunto del percorso sarà l'attività applicate. I partecpanti lavoreranno in gruppi per analizzare casi reali e redigere un documento finale condiviso.

I **gruppi di studio** saranno formati dalle Coordinatrici del corso in modo da garantire la massima eterogeneità delle professionalità e dei campi di specializzazione di ciascuno al fine di integrare visioni, metodi e competenze differenti.

L'elaborato, volto a proporre linee d'azione concrete per il settore della cybersecurity, sarà oggetto di una **presentazione ufficiale** agli stakeholder e alle istituzioni partner della Scuola.

Indicazioni sul calendario:

- Avvio del corso: previsto entro la **seconda metà di gennaio 2027**;

- Il calendario definitivo delle lezioni sarà pubblicato non appena raccolte tutte le conferme dei relatori e comunicato tempestivamente ai candidati e agli iscritti.

Art. 5 - PROGRAMMA DIDATTICO E MODULI

Il programma didattico della seconda edizione è strutturato in quattro moduli tematici interdisciplinari, volti a fornire una visione d'insieme del rapporto tra strategia, governance del rischio cyber, framework normativo e gestione operativa delle frodi. Ogni modulo integra l'analisi teorica con l'esame di casi studio d'eccellenza. Il corso, condotto in lingua italiana, si concentrerà sulle seguenti aree tematiche:

Modulo I — Strategia, Leadership e Geopolitica del Cyberspazio

Il cyberspazio come quinta dimensione della conflittualità, la postura strategica dell'Italia e dell'Unione Europea, il ruolo delle istituzioni preposte alla difesa del cyberspazio, il ruolo del CISO come figura di governance, il capitale umano e lo skills gap nel settore cyber.

Modulo II — Architettura Tecnica e Framework Normativo
I fondamenti della cybersicurezza, il modello NIST 2.0, la Direttiva NIS2 e il relativo recepimento italiano, il Regolamento DORA sulla resilienza operativa del settore finanziario, l'AI Act e la cybersicurezza dell'intelligenza artificiale, il quantum computing e la crittografia post-quantistica, la protezione delle infrastrutture critiche.

Modulo III — Cyber Fraud Management e Sicurezza Operativa
Il panorama delle frodi cibernetiche, il framework normativo antifrode (PSD2, PSD3), gli attacchi di tipo Business Email Compromise (BEC) e Man-in-the-Middle, l'Identity & Access Management e il modello Zero Trust, le indagini cyber e la digital forensics, la cyber insurance, la sicurezza della supply chain e la protezione delle PMI.

Modulo IV — Workshop Applicativo, Project Work e Valutazione
Simulazioni operative (tabletop exercise di incident response e simulazione di crisi cyber-diplomatica), elaborazione e discussione del Policy Paper finale davanti a un panel istituzionale, scenari cyber al 2030 e governance digitale globale, mercato del lavoro cyber e orientamento di carriera, Lectio Magistralis conclusiva con cerimonia di consegna dei diplomi.

Art. 6- BORSE DI STUDIO E QUOTE DI PARTECIPAZIONE

La selezione è aperta a cittadini italiani e stranieri residenti in Italia, lavoratori, laureati, dottorandi e ricercatori, manager del settore pubblico e privato i quali non abbiano compiuto il **quarantacinquesimo anno di età** alla data di scadenza del presente bando.

Il valore del corso è pari a **€ 5.000 (cinquemila).** Saranno ammessi i candidati che, previa selezione e colloquio, risulteranno vincitori di una borsa di studio a copertura totale o parziale.

Le borse di studio del presente bando sono così ripartite:

- **10 borse di studio a copertura totale** riservate a dottorandi e ricercatori;
- **20 borse di studio a copertura parziale** (dal 50% fino all'80% del costo totale di € 5.000).

La selezione si baserà su:

- Valutazione meritocratica dei curricula;

- Analisi delle condizioni economico-sociali (precarietà lavorativa, reddito, provenienza geografica svantaggiata).

L'assegnazione della borsa di studio a copertura parziale consente di diventare Sostenitore della Fondazione AISES, versando la quota residuale. Tale status darà diritto ad accedere, senza ulteriori costi, all'intera offerta formativa erogata dalla SPES Academy per l'anno accademico 2026/2027. Si rimanda all'Art. 11 del presente bando.

Art. 7 - DOMANDA DI AMMISSIONE E REGISTRAZIONE

Le candidature sono aperte a partire da venerdì 20 novembre 2026.

La domanda di ammissione dovrà pervenire entro e non oltre il giorno 11 gennaio 2027.

La richiesta va inviata esclusivamente via mail all'indirizzo

candidature.cybersecurity@spes.academy indicando come oggetto "Candidatura corso Cybersecurity e Gestione del Rischio Globale", completa dei seguenti allegati:

- Curriculum vitae in formato PDF;
- Fotografia in formato tessera;
- Lettera motivazionale.

Il curriculum dovrà contenere i seguenti elementi obbligatori:

- Dichiarazione dei propri dati anagrafici (nome, cognome, data e luogo di nascita, indirizzo di residenza e domicilio);
- Indicare un recapito telefonico e un valido indirizzo e-mail;
- Indicare facoltà, corso di laurea/post-laurea, sede, università;
- Indicare l'attuale principale occupazione, se presente.

La Commissione di valutazione si riserva la facoltà di procedere a idonei controlli sulla veridicità delle dichiarazioni sostitutive ai sensi del D.P.R. 28 dicembre 2000, n. 445.

Art. 8 - CAUSE DI ESCLUSIONE

Risulteranno prive di validità e non saranno prese in considerazione le domande che:

- perverranno oltre il termine specificato dall'Art. 7;

- saranno inviate a un indirizzo e-mail diverso da quello indicato all'Art. 7;
- risulteranno prive degli allegati obbligatori richiesti all'Art. 7;
- conterranno dichiarazioni mendaci.

Art. 9 - GRADUATORIA E CONFERMA DELL'ISCRIZIONE

La Commissione di valutazione formulerà l'elenco dei vincitori selezionati per titoli, merito e criteri sociali, **previa conduzione di un colloquio valutativo e conoscitivo.**

I vincitori del bando riceveranno comunicazione del giudizio della Commissione esaminatrice tramite e-mail. Al fine di garantire la corretta pianificazione amministrativa e l'eventuale scorrimento dei posti, i vincitori avranno a disposizione **3 giorni lavorativi** dalla ricezione della comunicazione per completare e confermare l'iscrizione attraverso il versamento della quota residuale.
Con l'iscrizione il partecipante si impegna ad accettare integralmente le disposizioni del presente bando. In caso di mancato riscontro o rinuncia entro il termine indicato, il posto sarà assegnato per scorrimento al primo dei candidati idonei inizialmente esclusi.

Art. 10 - TRATTAMENTO DEI DATI PERSONALI

Ai sensi del Regolamento (UE) 2016/679 («GDPR») e del D.lgs. 30 giugno 2003, n. 196 (così come modificato dal D.lgs. 10 agosto 2018, n. 101), i dati personali forniti dai candidati saranno trattati dalla Fondazione AISES ETS, in qualità di Titolare del trattamento, esclusivamente per le finalità connesse alla gestione della procedura di selezione, all'assegnazione delle borse di studio e all'organizzazione delle attività didattiche.

Il trattamento sarà effettuato nel rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione, esattezza, integrità e riservatezza, mediante strumenti cartacei e informatici idonei. I dati saranno conservati per il tempo strettamente necessario al perseguimento delle finalità di selezione e, per i candidati ammessi, per il periodo richiesto dagli obblighi normativi e contabili applicabili. Restano salve le disposizioni sull'accesso di cui alla legge n. 241/90 e successive modificazioni.

Art. 11 - ATTIVITÀ INTEGRATIVE ED ACCESSO ESTESO

Tutti i partecipanti ammessi al Corso di Alta Formazione che avranno conseguito lo status di Sostenitore della Fondazione AISES ETS avranno diritto di **accesso gratuito a tutte le attività**

formative parallele, ai Corsi di Alta Formazione, ai seminari speciali e ai moduli integrativi organizzati dalla SPES Academy nel corso dell'anno accademico 2026/2027.

Le modalità di partecipazione, i contenuti opzionali e il calendario dettagliato di tali attività saranno tempestivamente comunicati agli iscritti a cura della Segreteria Organizzativa.