Corso intensivo nella Cyber Resilience ed esame di certificazione

(Codice: CRP501)

Durata: 16 ore di lezione distribuite in due giorni; esame online di certificazione al termine del corso oppure in autonomia a scelta del partecipante

Esame: Esame di Certificazione Professionale DRI International nella Cyber Resilience

Costo, iscrizione e ulteriori informazioni: Il costo del corso CRP501 in Italia nel 2025 è fissato in 1.600 euro + IVA.

Incluso nel costo del corso

- Corso online o in presenza erogato in italiano da docenti certificati DRI
- Materiale del corso in inglese e in formato digitale
- Attestato di partecipazione
- Esame di qualificazione alla certificazione, online, in inglese

Descrizione del corso

Le organizzazioni si trovano oggi ad affrontare un'ampia gamma di attacchi informatici e la vostra organizzazione non fa eccezione. Gli hacker hanno innumerevoli possibilità di provocare gravi disfunzioni, che richiedono una risposta che coinvolge anche chi si occupa di BCM e Risk Management. Questo corso è adatto sia a chi ha almeno due anni di esperienza nella cyber security o information security e desidera ottenere la prestigiosa certificazione **CCRP (Certified Cyber Resilience Professional)**, sia a chi vuole dedicare un tempo limitato alla materia e quindi apprenderne gli elementi fondamentali giungendo comunque alla certificazione di primo livello **ACRP (Associate Cyber Resilience Professional)**. Questo non è un corso tecnico per specialisti della cyber security, ma finalizzato a illustrare come le organizzazioni possano integrare i concetti di continuità operativa nella cyber security e viceversa per soddisfare i requisiti del business. Verranno utilizzati e sintetizzati i cinque elementi principali dei framework di cyber security: identificazione, protezione, rilevamento, risposta e recupero. Nel complesso, questi concetti e i piani d'azione che ne derivano aiuteranno a sviluppare una strategia per rispondere efficacemente agli eventi imprevisti e riportare l'organizzazione in funzione il più rapidamente possibile. Queste due discipline, BCM e Cybersecurity, spesso separate all'interno delle aziende, possono lavorare insieme e, grazie a questo corso, sarete in grado di far sì che ciò accada nella vostra organizzazione. In questo modo, si semplificherà l'identificazione e la risposta ben coordinata agli attacchi o alle violazioni dei dati, si ridurranno al minimo i costi, si proteggerà la reputazione dell'organizzazione e si otterrà il vantaggio professionale di portare al tavolo della Direzione le informazioni e le competenze più aggiornate. Al superamento dell'esame, possibilità di richiedere subito la certificazione di primo livello come **Associate Cyber Resilience Professional (ACRP)**. Per la certificazione di livello superiore **Certified Cyber Resilience Professional (CCRP)**, è necessaria la dimostrazione di possesso dei requisiti di esperienza professionale almeno biennale. L'emissione della certificazione richiede il pagamento di una quota una-tantum direttamente sul sito www.drii.org

DRI International

DRI Italy

Obiettivo

1. Fornire agli studenti un quadro di riferimento e una guida per l'implementazione dei concetti essenziali per combinare la cyber security e la continuità operativa (BCM) in un programma efficace di Cyber Resilience
2. Fornire agli studenti gli elementi per presentare un'appropriata "proposta di valore" al senior management di un'organizzazione, con la finalità di garantire il loro appoggio al varo di un solido programma di Cyber Resilience
3. Preparare gli studenti a superare l'esame finale di Cyber Resilience, in modo da essere certificati da DRI International come ACRP o CCRP.

Struttura del corso

Lezione 1

- Introduzione al concetto di Cyber Resilience e sicurezza informatica
- Tipi di eventi cyber
- Come gli eventi di cybersecurity impattano sulla continuità aziendale
- Integrazione della cybersecurity nella continuità operativa (BC)
- Considerazioni organizzative
- Passare dalla cybersecurity e dal Business Continuity Management per raggiungere la Cyber Resilience
- Sviluppare una risposta efficace agli incidenti
- Identificare strumenti specifici per unire la pianificazione della risposta agli incidenti di cybersecurity e la pianificazione della continuità aziendale (BCM)
- Progettare strategie che mitighino i danni in caso di violazione dei sistemi
- Identificare i parametri critici delle operazioni legate all'IT per una corretta valutazione dell'impatto sull'organizzazione
- Elencare le strategie di ripristino dei sistemi cruciali per recuperare la tecnologia e la continuità dei processi critici dell'organizzazione
- Vantaggi dell'identificazione dei rischi informatici e della loro integrazione nella pianificazione e gestione dell'azienda

Lezione 2

- Creare un sistema di gestione per la cybersecurity
- Presentazione del più diffuso sistema di riferimento per la cybersecurity
- Presentazione delle normative esistenti che regolano la protezione e la gestione della sicurezza informatica
- Come sviluppare e implementare la protezione delle infrastrutture e dei servizi tecnologici critici per contenere l'impatto di un attacco informatico
- Come rilevare e monitorare gli indicatori di attacco alla rete e garantire l'efficacia delle protezioni
- Descrivere l'importanza di una formazione regolare sulla consapevolezza informatica.
- Monitorare gli eventi di sicurezza interni e correlarli alle minacce esterne
- Creare un piano di risposta efficace
- Come ripristinare i dati e i servizi che potrebbero essere stati danneggiati durante un attacco informatico
- Comprendere come la Cybersecurity e la Business Continuity dell'azienda lavorino entrambe per

la protezione della reputazione e immagine aziendale
- Monitoraggio della cybersecurity
- Creare piani di comunicazione di crisi efficaci per gli incidenti informatici
- Elencare le raccomandazioni per preparare i fornitori chiave in caso di cyber attack
- Discutere come le iniziative di formazione e sensibilizzazione del personale dovrebbero essere utilizzate per incorporare la resilienza informatica all'interno dell'organizzazione e garantire che il personale conosca la funzione dei piani di risposta all'incidente.

Modalità di erogazione del corso

Corsi pubblici

Questi corsi sono aperti a tutti, e sono erogati online oppure in presenza: verifica il calendario dei corsi disponibili in Italia sul sito www.dri-italy.it

Corsi privati
Le Aziende, le Associazioni, gli Enti Pubblici che desiderano formare più dipendenti, soci o collaboratori, possono richiedere alla segreteria@dri-italy.it la quotazione di un corso privato, che sarà erogato negli orari e nelle sedi preferite dall'acquirente.

Certificazioni

Il corso consente agli studenti di sostenere l'esame di certificazione e – in caso di successo – acquistare in seguito direttamente sul sito di DRI International www.drii.org il certificato richiesto (ACRP, CCRP).

Tutte le certificazioni richiedono il pagamento di una quota una-tantum NON inclusa nel costo del corso, pagabile tramite carta di credito sul sito www.drii.org.

I costi una-tantum nel 2025 sono i seguenti:

- ACRP: 200 USD
- CCRP: 400 USD

Certificazione ACRP (Associate Cyber Resilience Professional)

La certificazione ACRP non ha altri requisiti oltre al superamento dell'esame finale.

Certificazioni CCRP (Certified Cyber Resilience Professional)

Il candidato che dispone di più di due anni di esperienza in ambito Cyber può richiedere, dopo il superamento dell'esame, un livello di certificazione superiore a quello ACRP. Le esperienze professionali devono essere dimostrate fornendo una serie di informazioni in fase di richiesta.