Corso approfondito nella Cyber Resilience e certificazione

(Codice: CRLE 2000)

Durata: 4,5 giorni (quattro giorni interi di lezione dalle 9:00 alle 18:00; esame il quinto giorno dalle 9:00 alle 13:00, oppure dalle 14:00 alle 17:00).

Esame: Esame di Certificazione Professionale DRI International nella Cyber Resilience

Costo, iscrizione e ulteriori informazioni: Il costo del corso CRLE2000 in Italia nel 2024 è fissato in 2.600 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 certificazione, online, in italiano o in inglese
- Certificazione di primo livello ACRP, Associate Cyber Resilience Professional. (Richiede solo il superamento dell'esame)
- **Per la certificazione di livello superiore** CCRP, è necessario il superamento dell'esame di cui sopra nonché il versamento di una quota aggiuntiva e la dimostrazione di possesso dei requisiti di esperienza professionale biennale (tramite la compilazione di un modulo specifico).

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. Ecco perché questo corso è assolutamente necessario per Voi. Più che una semplice esposizione del problema, il corso Cyber Resilience è un'esperienza di quattro giorni ricca di informazioni che vi permetterà di capire come affrontare le interruzioni informatiche all'interno di un quadro di continuità aziendale. Questo non è un corso tecnico per specialisti della cyber security, ma finalizzato a scoprire come la continuità operativa e la cyber security debbano integrarsi in ogni organizzazione. Verranno utilizzati 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, devono 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 cyber 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 sul tavolo della Direzione le

informazioni e le competenze più aggiornate.

Obiettivo

1. Fornire agli studenti istruzioni dettagliate, 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. Preparare gli studenti con raccomandazioni attuabili per rappresentare un'appropriata "proposta di valore" al management di un'organizzazione, con la finalità di garantire qualsiasi investimento necessario per varare un solido programma di Cyber Resilience
3. Prepararsi a superare l'esame finale di Cyber Resilience, in modo da essere certificati da DRI International come **ACRP**, **Associate Cyber Resilience Professional** oppure **CCRP, Certified Cyber Resilience Professsional**.

Struttura del corso

GIORNO 1

- Introduzione al concetto di Cyber Resilience e resilienza informatica
- Tipi di eventi informatici
- 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

GIORNO 2

- 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
- 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

GIORNO 3

- 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

GIORNO 4

- 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.

Certificazione ACRP (Associate Cyber Resilience Professional)

Il corso consente agli studenti di sostenere l'esame di certificazione e – in caso di successo – ottenere il certificato ACRP. Il tutto incluso nel costo concordato. La certificazione ACRP non ha altri requisiti oltre al superamento dell'esame finale.

Certificazione CCRP (Certified Cyber Resilience Professional)

Il candidato che considera di disporre dei requisiti di esperienza richiesti, può richiedere già al momento dell'iscrizione al corso il livello di certificazione superiore **CCRP**, con un modesto costo addizionale. Tuttavia, il certificato CCRP richiede più di due (2) anni di esperienza che devono essere dimostrati tramite un apposito modulo dopo il superamento dell'esame.

Se avete meno di due anni di esperienza nel settore, potete richiedere solo la certificazione ACRP, già incluso nel costo del corso.

Modalità di erogazione del corso

Corsi pubblici a calendario DRI Italy

Questi corsi sono aperti a tutti, e sono erogati online oppure in presenza: verifica il calendario dei corsi disponibili in Italia

Per i corsi in presenza:

Il corso si tiene dalle 9 alle 18 presso la città e la sede indicata. L'esame si tiene la mattina oppure il pomeriggio del quinto giorno. Per questo corso è consigliato disporre di un computer ed è comunque necessario per poter sostenere l'esame. I requisiti di sistema vi saranno inviati via e-mail insieme alle informazioni su come accedere al materiale didattico prima dell'inizio del corso.

Per i corsi online:

Tutti i corsi online si tengono tramite GoToMeeting, Microsoft Teams o soluzioni similari e per questo è necessario un computer connesso a Internet. I requisiti di sistema vi saranno inviati via e-mail insieme alle informazioni su come accedere al materiale didattico prima dell'inizio del corso. Verranno inoltre fornite le istruzioni per sostenere l'esame online dopo il corso.

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.