Catalogo dei

Corsi DRI Italy
e
Corsi Continuitaly

2024

Sommario

Corsi DRI Italy

Corso intensivo nel Business Continuity Management e certificazione (codice: BCP501)

Durata: 2,5 giorni (due giorni interi di lezione dalle 9:00 alle 18:00; esame il terzo giorno dalle 9:00 alle 13:00, oppure dalle 14:00 alle 17:00).

Esame: Esame di Certificazione Professionale DRI International nel Business Continuity Management

Costo, iscrizione e ulteriori informazioni: Il costo del corso BCP501 in Italia nel 2024 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 certificazione, online, in italiano o in inglese
- Certificazione di primo livello ABCP, Associate Business Continuity Professional. (Richiede solo il superamento dell'esame)
- **Per le certificazioni di livello superiore** CBCV e CBCP, 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

Un'incredibile quantità di informazioni è racchiusa in questo corso dal ritmo incalzante, pensato sia per chi è già un esperto di continuità aziendale, e vuole sostenere l'esame finale per accedere alla certificazione internazionale come **Business Continuity Professional**, sia per chi ha poco tempo e vuole acquisire una preparazione più che sufficiente nella materia. Se avete fretta di portare la vostra carriera al livello successivo, il corso intensivo BCP 501 fa per voi. Questo corso, breve ma molto efficace, vi farà conoscere gli elementi chiave della continuità operativa, e la corretta terminologia. Il corso si basa sulle **DRI Professional Practices for Business Continuity Management**, le linee guida più utilizzate e collaudate del settore. Tutti gli standard internazionali sul BCM hanno le fondamenta nelle Pratiche Professionali definite più di 50 anni fa da DRI. Il docente certificato DRI si concentra sul fornire anche gli strumenti necessari per superare l'esame di qualificazione, che è il primo passo per la certificazione come **Associate Business Continuity Professional (ABCP)**, **Certified Business Continuity Professional (CBCP)** o come **Certified Business Continuity Vendor (CBCV)**

Obiettivi del corso

1. Esaminare il corpus di conoscenze costituito dalle Professional Practices for Business Continuity

Management, progettato per assistere nello sviluppo, nell'implementazione e nel mantenimento dei programmi di continuità aziendale (BCM Program).

2. Evidenziare i termini e le metodologie presentate nel Glossario internazionale per la resilienza e nelle Pratiche Professionali DRI.
3. Preparare il candidato all'esame di certificazione.

Struttura del corso

Giorno 1

Lezione 1: Avvio e gestione del programma

- Stabilire la necessità di un programma di continuità operativa.
- Ottenere supporto e finanziamenti per il programma di continuità operativa.
- Costruire il quadro organizzativo a supporto del programma di continuità operativa.
- Introdurre i concetti chiave, come la gestione del programma, la consapevolezza del rischio, l'identificazione delle funzioni/processi critici, le strategie di ripristino, la formazione e la sensibilizzazione e le esercitazioni/test.

Lezione 2: Risk Assessment (Valutazione del rischio)

- Identificare i rischi che possono influire negativamente sulle risorse o sull'immagine di una organizzazione.
- Valutare i rischi e determinare gli impatti potenziali sull'organizzazione, consentendo all'organizzazione di determinare l'uso più efficace delle risorse per ridurre tali impatti potenziali.

Lezione 3: Business Impact Analysis (Analisi dell'impatto sul business)

- Identificare e dare priorità alle funzioni e ai processi dell'organizzazione per verificare quali avranno il maggiore impatto nel caso in cui non siano disponibili.
- Valutare le risorse necessarie per supportare il processo di BIA.
- Analizzare i risultati per accertare eventuali lacune tra i requisiti dell'organizzazione e la sua capacità di soddisfarli.

Lezione 4: Strategie di continuità aziendale

- Selezionare strategie efficaci, anche dal punto di vista dei costi, per ridurre le carenze identificate durante i processi di valutazione dei rischi e di BIA.

Lezione 5: Risposta agli incidenti (Incident Response)

- Sviluppare e assistere l'organizzazione nell'implementazione di un sistema di gestione degli incidenti che definisca ruoli organizzativi, linee di comando e processi di escalation.
- Definire i requisiti per sviluppare e implementare il piano di risposta agli incidenti dell'organizzazione. Garantire che la risposta agli incidenti sia coordinata con organizzazioni

esterne in modo tempestivo ed efficace, se necessario.

Giorno 2

Lezione 6: Sviluppo e attuazione dei piani (Business Continuity Plan, BCP)

- Documentare i piani da utilizzare durante un incidente che consentiranno all'organizzazione di continuare a funzionare.

Lezione 7: Programmi di sensibilizzazione e formazione

- Stabilire e mantenere programmi di formazione e sensibilizzazione che portino il personale a rispondere agli incidenti in modo calmo ed efficiente.

Lezione 8: Esercitazione, verifica e manutenzione del piano di continuità aziendale

- Stabilire un programma di esercitazione, valutazione e manutenzione per mantenere uno stato di prontezza.

Lezione 9: Comunicazioni di crisi

- Fornire un quadro di riferimento per lo sviluppo di un piano di comunicazione di crisi.
- Garantire che il piano di comunicazione di crisi preveda una comunicazione tempestiva ed efficace con le parti interne ed esterne.

Lezione 10: Coordinamento con le autorità

- Stabilire politiche e procedure per coordinare le attività di risposta agli incidenti con gli enti pubblici.

Lezione 11: Ripasso in vista dell'esame di qualificazione alla certificazione

- Rivedere i concetti importanti di ciascuna delle lezioni precedenti.
- Preparatevi per l'esame di qualificazione attraverso una revisione delle domande dell'esame pratico.

Corso approfondito nel Business Continuity Management e certificazione (Codice: BCLE2000)

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 nel Business Continuity Management

Costo, iscrizione e ulteriori informazioni: Il costo del corso BCLE2000 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 ABCP, Associate Business Continuity Professional. (Richiede solo il superamento dell'esame)
- **Per le certificazioni di livello superiore** CBCV e CBCP, 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

Il corso vi permette di costruire, gestire e migliorare un programma di continuità aziendale (BCM) basato sulle metodologie più aggiornate e sullo standard più utilizzato e collaudato nel tempo, perché le ***Professional Practices for Business Continuity Management*** (Prassi Professionali per il BCM) di DRI International sono proprio questo. Da tempo standard di riferimento per la nostra professione, le Professional Practices sono le fondamenta su cui si basa questo corso di quattro giorni, approfondito e pratico. Tutti gli standard internazionali sul BCM hanno le fondamenta nelle Prassi Professionali per il BCM definite più di 50 anni fa da DRI. Il corso include tutte le dieci Professional Practices Professionali descritte di seguito, aggiornate negli anni considerando le nuove condizioni che vivono le aziende quali il cloud computing, le minacce cyber, i rischi della catena di fornitura (supply chain), le soluzioni assicurative per il trasferimento del rischio, oltre ad argomenti più tradizionali come la valutazione dei rischi (Risk Assessment), come fare a guadagnare l'appoggio della leadership, le tecniche comunicazione in condizione di crisi, la revisione ed aggiornamento continuo del programma di BCM. Un docente esperto, certificato da DRI International, vi guiderà attraverso gli elementi chiave della gestione della continuità operativa utilizzando esempi del mondo reale ed esercizi interattivi, rendendo questo corso

perfetto per coloro che sono relativamente nuovi alla professione e desiderano un'esperienza formativa approfondita, senza lasciare nulla di inesplorato. La natura partecipativa del corso vi immerge nel processo di apprendimento, vi permette di imparare facendo e vi assicura di lasciare il corso avendo acquisito una solida base per costruire o migliorare il vostro programma di BCM specifico per la vostra organizzazione. Inoltre, il corso e il materiale di supporto fornito a ogni studente sono progettati per fornire tutti gli strumenti necessari per superare l'esame di certificazione e ottenere il certificato **Associate Business Continuity Professional (ABCP) (compreso nel costo del corso)** oppure richiedere i certificati di livello superiore, **Certified Business Continuity Vendor (CBCV)** oppure **Certified Business Continuity Professional (CBCP),** sulla base delle esigenze e dei requisiti di esperienza personali.

Allineamento e approfondimento sullo standard ISO22301
Lo standard ISO22301 è largamente utilizzato nel nostro Paese dalle aziende che intendono dotarsi di un sistema di gestione della continuità operativa. Sebbene questo corso DRI sia incentrato sulle Professional Practices DRI, una intera lezione del corso è dedicata all'esame dello standard ISO22301 e alla verifica incrociata con le Professional Practices, che sono sempre applicabili per il soddisfacimento dei requisiti dello standard stesso.

Obiettivi del corso

4. Esaminare il corpus di conoscenze costituito dalle Professional Practices for Business Continuity Management, progettato per assistere nello sviluppo, nell'implementazione e nel mantenimento dei programmi di continuità aziendale.
5. Evidenziare i termini e le metodologie presentate nel Glossario internazionale per la resilienza e nelle Pratiche Professionali.
6. Preparare il candidato all'esame di certificazione.

Struttura del corso

Lezione 1: Avvio e gestione del programma

- Stabilire la necessità di un programma di continuità operativa.
- Ottenere supporto e finanziamenti per il programma di continuità operativa.
- Costruire il quadro organizzativo a supporto del programma di continuità operativa.
- Introdurre i concetti chiave, come la gestione del programma, la consapevolezza del rischio, l'identificazione delle funzioni/processi critici, le strategie di ripristino, la formazione e la sensibilizzazione e le esercitazioni/test.
- ***Esercizio in classe:*** Predisposizione di una presentazione per la leadership sull'importanza della continuità operativa, sui requisiti legali e normativi pertinenti, sui requisiti delle risorse del progetto e su una panoramica del piano di progetto con fasi ben definite.

Lezione 2: Risk Assessment (Valutazione del rischio)

- Identificare i rischi che possono influire negativamente sulle risorse o sull'immagine di una organizzazione.
- Valutare i rischi e determinare gli impatti potenziali sull'organizzazione, consentendo all'organizzazione di determinare l'uso più efficace delle risorse per ridurre tali impatti potenziali.
- ***Esercizio in classe***: Predisposizione di una presentazione per la leadership che identifichi tre minacce significative, determini quali controlli sono attualmente in atto per queste minacce e le vostre raccomandazioni per migliorare i controlli attuali o implementare nuovi controlli per ciascuna minaccia; sviluppare una bozza del rapporto finale di valutazione del rischio.

Lezione 3: Business Impact Analysis (Analisi dell'impatto sul business)

- Identificare e dare priorità alle funzioni e ai processi dell'organizzazione per verificare quali avranno il maggiore impatto nel caso in cui non siano disponibili.
- Valutare le risorse necessarie per supportare il processo di BIA.
- Analizzare i risultati per accertare eventuali lacune tra i requisiti dell'organizzazione e la sua capacità di soddisfarli.
- ***Esercizio in classe:*** Sviluppare un elenco prioritizzato di funzioni e processi aziendali, la criticità di ciascuna funzione e processo aziendale, e i relativi RTO, RPO.

Lezione 4: Strategie di continuità aziendale

- Selezionare strategie efficaci, anche dal punto di vista dei costi, per ridurre le carenze identificate durante i processi di valutazione dei rischi e di BIA.
- ***Esercizio in classe:*** Basatevi sugli esercizi precedenti per identificare le strategie di continuità/recupero, includendo una breve descrizione, i vantaggi e gli svantaggi e una stima dei costi di ciascuna strategia. Discutete come presentereste le raccomandazioni per ottenere l'approvazione della leadership.

Lezione 5: Risposta agli incidenti (Incident Response)

- Sviluppare e assistere l'organizzazione nell'implementazione di un sistema di gestione degli incidenti che definisca ruoli organizzativi, linee di comando e processi di escalation.
- Definire i requisiti per sviluppare e implementare il piano di risposta agli incidenti dell'organizzazione. Garantire che la risposta agli incidenti sia coordinata con organizzazioni esterne in modo tempestivo ed efficace, se necessario.
- ***Esercizio in classe:*** Identificare le azioni necessarie per rispondere agli eventi, elencare la formazione speciale necessaria, determinare il tipo di piano necessario ed elencare le azioni correttive da applicare subito per consentire la risposta agli incidenti.

Lezione 6: Sviluppo e attuazione dei piani (Business Continuity Plan, BCP)

- Documentare i piani da utilizzare durante un incidente che consentiranno all'organizzazione di continuare a funzionare.
- ***Esercizio in classe:*** Identificare il tipo di piano di continuità aziendale (BCP) necessario per

l'azienda, definire l'ambito, gli obiettivi e i prerequisiti del piano. Determinare le informazioni da raccogliere e il suo ruolo nell'ambito del programma complessivo di continuità aziendale.

Lezione 7: Programmi di sensibilizzazione e formazione

- Stabilire e mantenere programmi di formazione e sensibilizzazione che portino il personale a rispondere agli incidenti in modo calmo ed efficiente.
- ***Esercizio in classe:*** Sviluppare un programma di formazione e informazione per i responsabili del piano e gli altri impiegati, che includa i temi vitali della formazione, la frequenza dei corsi, il processo di selezione del personale da formare/informare e altre raccomandazioni per consentire la risposta alle emergenze.

Lezione 8: Esercitazione, verifica e manutenzione del piano di continuità aziendale

- Stabilire un programma di esercitazione, valutazione e manutenzione per mantenere uno stato di prontezza.
- ***Esercizio in classe:*** Sviluppare uno scenario di esercitazione/test rilevante per la propria organizzazione, valutare le risorse necessarie, ciò che verrà esercitato/testato e descrivere i passi da seguire per metterlo in atto.

Lezione 9: Comunicazioni di crisi

- Fornire un quadro di riferimento per lo sviluppo di un piano di comunicazione di crisi.
- Garantire che il piano di comunicazione di crisi preveda una comunicazione tempestiva ed efficace con le parti interne ed esterne.
- ***Esercizio in classe:*** Discutere in classe sul processo da mettere in atto per determinare se un evento è una crisi potenziale, la natura della crisi, le parti interessate, i portavoce e il messaggio chiave per i media.

Lezione 10: Coordinamento con le autorità

- Stabilire politiche e procedure per coordinare le attività di risposta agli incidenti con gli enti pubblici.

Lezione 10A: Confronto con ISO22301

- Introduzione allo standard ISO22301 sue finalità, differenze e analogie con le Professional Practices DRI
- Presentazione della matrice di conversione tra ISO22301 e Professional Practices DRI.

Lezione 11: Ripasso in vista dell'esame di qualificazione alla certificazione

- Rivedere i concetti importanti di ciascuna delle lezioni precedenti.
- Preparatevi per l'esame di qualificazione attraverso una simulazione delle domande dell'esame.

Certificazione inclusa nel corso dei Corsi BCP501 e BCLE2000

Certificazione ABCP (Associate Business Continuity Professional)

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

Certificazioni di livello superiore (richiedono quota aggiuntiva)

Certificazioni CBCP (Certified Business Continuity Professional) e CBCV (Certified Business Continuity Vendor)

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

Requisiti per certificazione CBCV

La certificazione CBCV è rivolta a persone che forniscono consulenza, servizi e prodotti nell'ambito della BCM e DR e hanno così acquisito almeno due (2) anni di esperienza generale nella continuità operativa. Questa certificazione richiede il pagamento di una quota addizionale.

Requisiti per certificazione CBCP

La certificazione CBCP è rivolta a persone che hanno una discreta conoscenza ed esperienza lavorativa nel settore della continuità operativa e/o disaster recovery. Il livello CBCP richiede più di due (2) anni di esperienza; i candidati devono essere in grado di dimostrare un'esperienza in cinque (5) delle aree tematiche delle Pratiche Professionali DRI. Questa certificazione richiede il pagamento di una quota addizionale.

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

Corso IT Disaster Recovery Planning
(codice: ITDRP)

Durata: 2 giorni (due giorni interi di lezione dalle 9:00 alle 18:00; esame di verifica dell'apprendimento al termine al termine del corso)

Esame: non è previsto un esame di certificazione, solo di verifica dell'apprendimento. Nota Bene: Chi segue la stessa settimana anche il corso BCP501 sosterrà l'esame di qualificazione al suo termine (vedi scheda BCP501)

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

Descrizione

Mai prima d'ora, nella storia, la nostra fiducia nell'automazione è stata maggiore. E mai prima d'ora abbiamo visto così tante minacce ai sistemi informativi e ai dati da cui dipendiamo. La risposta migliore consiste nella implementazione di un completo sistema di IT Disaster Recovery Planning, integrato nel sistema aziendale di Business Continuity Management. Con il corso di formazione **IT Disaster Recovery Planning** di DRI, scoprirete i vantaggi e gli svantaggi degli strumenti e dei processi a disposizione e come la vostra organizzazione può aumentare la propria resilienza. Si suggerisce di frequentare in aggiunta al presente corso anche il **corso intensivo sul Business Continuity Management BCP501**, comprensivo dell'esame di qualificazione alla certificazione, per approfondire le tematiche di BCM e accedere al percorso di certificazione professionale DRI International.

Obiettivi del Corso

1. Comprendere la struttura dei sistemi di gestione della continuità operativa (BCM)
2. Imparare il ruolo dell'IT DRP all'interno del BCM
3. Riconoscere i problemi legati al recupero della funzionalità delle piattaforme tecnologiche e dei dati
4. Valutare le tecnologie IT e DR attuali ed emergenti
5. Selezionare alternative strategiche per il processo IT DRP
6. Costruire, testare e implementare il processo di IT DRP
7. Integrare le funzioni BCM e IT DRP all'interno dell'azienda
8. Apprendere le conoscenze contenute nelle Professional Practices for Business Continuity Management DRI (pratiche professionali per la gestione della continuità aziendale) progettate da DRI per assistere le organizzazioni nello sviluppo, implementazione e manutenzione dei

programmi di continuità aziendale

9. Apprendere i termini e le metodologie raccolte da DRI nel Glossario Internazionale per la Resilienza e le Prassi Professionali

Struttura del corso

Lezione 1: Come creare il piano del progetto IT DRP e ottenere l'approvazione della direzione aziendale

- Definire obiettivi
- Determinazione dei risultati
- Approvazione della Direzione
- Esercizio: Sviluppare un piano di progetto IT DRP

Lezione 2: Esecuzione della valutazione dei rischi (Risk Assessment) e dell'analisi dell'impatto sul business (BIA)

- Valutazione del rischio e BIA (breve discussione)
- Requisiti dell'area di business e interdipendenze con l'IT (applicazioni, archiviazione dati, rete, sistemi, ecc.)
- Obiettivi di recupero (RTO e RPO)
- Assegnazione delle priorità alle applicazioni, ai server e ai sistemi in accordo a RTO e RPO
- Esercizio: Sviluppare un documento BIA specifico per l'IT

Lezione 3: Selezione di una strategia IT DRP

- Backup dei dati e opzioni di ripristino
- Opzioni di ripristino di sistemi e piattaforme
- Opzioni di ripristino della rete
- Esercizio: Sviluppare un documento sulle strategie IT

Lezione 4: Sviluppo del documento IT DRP

- Indice dei contenuti
- Esercizio: Sviluppare un IT DRP

Lezione 5: Introduzione alle nuove tecnologie IT DRP e al loro impatto sui tempi di recupero (RTO)

- Il ruolo dello specialista DR
- Panoramica delle tecnologie DR
- Ambienti e centri dati
- Cloud computing e reti
- Gestione di DR e ambienti virtuali
- Esercizio: Definire una tecnica di recupero, formulare una strategia di pianificazione del recupero e fornire un'analisi costi/benefici. Sviluppo dell'indice dei contenuti del piano IT/DR

Corso intensivo nella Cyber Resilience e certificazione (Codice: CRP501)

Durata: 2,5 giorni (due giorni interi di lezione dalle 9:00 alle 18:00; esame il terzo 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 CRP501 in Italia nel 2024 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 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. 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.

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

GIORNO 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

GIORNO 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.

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

DRI Italy

Continuitaly

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 inclusa nel corso dei corsi CRLE2000 e CRP501

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 di livello superiore che richiede il versamento di una quota aggiuntiva

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.

Corsi Continuitaly

DRI Italy

Continuitaly

Workshop pratico di implementazione del Business Continuity Management in accordo allo standard ISO22301

Durata: 2 giorni di lezione dalle 9:00 alle 18:00
Esame: non previsto
Incluso nel costo del corso

- Corso online o in presenza erogato in italiano o inglese
- Materiale del corso in italiano o inglese e in formato digitale
- Attestato di partecipazione

Descrizione
Il workshop pratico di implementazione dello standard ISO 22301 sul business continuity management è un'opportunità per le organizzazioni di formare al meglio le risorse dedicate a sviluppare un piano di continuità aziendale robusto e affidabile, in grado di far fronte alle situazioni di crisi che possono verificarsi. Il workshop prevede l'incontro e la collaborazione tra gli studenti, più o meno competenti nell'ambito del BCM e il docente, dotato di competenze specifiche in materia di business continuity, con l'obiettivo di sviluppare in due giorni un piano di continuità aziendale sulla base dello standard ISO 22301.
Di seguito sono riportate le attività incluse nel workshop, che prendono l'avvio dall'analisi di un caso di studio, che descrive una ipotetica azienda nella quale implementare un sistema di BCM.

- Analisi dei rischi: i partecipanti del workshop dovrebbero svolgere un'analisi dei rischi per identificare le minacce che potrebbero interrompere le attività dell'organizzazione e determinare la loro probabilità e l'impatto potenziale. Questa analisi dovrebbe servire da base per il piano di continuità aziendale.
- Definizione degli obiettivi e delle priorità: una volta identificati i rischi, i partecipanti definiscono gli obiettivi del piano di continuità aziendale e stabiliscono le priorità per le attività di ripristino in accordo ai risultati della Business Impact Analysis;
- Identificazione delle responsabilità: i partecipanti individuano ruoli e responsabilità per la gestione del piano di continuità aziendale e per la risposta alle emergenze;
- Pianificazione delle attività di continuità aziendale: i partecipanti definiscono il piano (business continuity plan) che dettaglia le attività necessarie per garantire la continuità delle attività dell'organizzazione in caso di interruzione e stabiliscono i tempi di attuazione.
- Definizione del piano di comunicazione: i partecipanti definiscono il piano di comunicazione per la gestione delle emergenze e per la comunicazione interna ed esterna.
- Esercitazioni e simulazioni: il workshop prevede la definizione di un programma di esercitazioni e simulazioni per testare la validità del piano di continuità aziendale e migliorarne l'efficacia.
- Valutazione e miglioramento continuo: i partecipanti definiscono le modalità con le quali valutare regolarmente l'efficacia del piano di continuità aziendale e identificare le aree di miglioramento.

Durante il workshop, gli istruttori guidano i partecipanti nell'implementazione dello standard ISO 22301 e fornire supporto e consulenza sui punti critici della pianificazione della continuità aziendale. Gli istruttori sono esperti in materia di business continuity e hanno una solida conoscenza dello standard ISO 22301, oltre a competenze nella gestione delle emergenze e nella gestione dei rischi.

DRI Italy

Continuitaly

Il workshop dovrebbe durare almeno due giorni per consentire ai partecipanti di acquisire le competenze necessarie per implementare il piano di continuità aziendale. Inoltre, il workshop dovrebbe prevedere un follow-up con l'organizzazione per monitorare l'implementazione del piano di continuità aziendale e fornire ulteriore supporto e consulenza, se necessario.

Struttura del corso

Il corso prevede un'alta componente pratica, basata sull'utilizzo di un case study che permette di simulare scenari reali e di applicare concretamente i concetti teorici presentati. Gli studenti lavoreranno in gruppo e avranno modo di confrontarsi con colleghi provenienti da diverse organizzazioni e settori, favorendo lo scambio di esperienze e di best practices. Gli istruttori sono esperti del settore e forniranno un supporto continuo durante le esercitazioni pratiche e le attività di gruppo. Al termine del corso, gli studenti avranno acquisito le competenze e gli strumenti necessari per sviluppare e implementare un sistema di business continuity management basato sullo standard ISO 22301.

Primo giorno

Sessione 1: Introduzione al business continuity management e allo standard ISO 22301

- Presentazione del corso e degli obiettivi
- Introduzione al business continuity management e ai concetti chiave
- Panoramica dello standard ISO 22301
- Presentazione del case study utilizzato per sviluppare e implementare un sistema di business continuity management

Sessione 2: Analisi del contesto e valutazione dei rischi

- Identificazione dei fattori di rischio interni ed esterni
- Analisi dell'impatto delle interruzioni sulle attività aziendali
- Valutazione dei rischi e delle opportunità di miglioramento
- Utilizzo del case study per sviluppare l'Analisi del contesto e valutazione dei rischi

Sessione 3: Pianificazione e implementazione del business continuity management

- Definizione della strategia di business continuity management
- Pianificazione delle attività di business continuity management
- Implementazione del piano di business continuity management
- Utilizzo del case study per sviluppare la fase di Pianificazione e implementazione del business continuity management

Secondo giorno

Sessione 4: Risposta alle emergenze e ripristino delle attività

- Definizione delle attività di risposta alle emergenze

- Pianificazione del ripristino delle attività aziendali
- Attività post-crisi e gestione delle conseguenze
- Utilizzo del case study per sviluppare la fase di Risposta alle emergenze e ripristino delle attività

Sessione 5: Monitoraggio, valutazione e miglioramento del sistema di business continuity management

- Monitoraggio delle prestazioni del sistema di business continuity management
- Valutazione dei risultati e miglioramento continuo
- Implementazione di azioni correttive
- Utilizzo del case study per sviluppare la fase di Monitoraggio, valutazione e miglioramento del sistema

Sessione 6: Formazione, esercitazioni, test

- Sviluppo di un programma di formazione e test
- Progettazione di simulazioni e esercitazioni
- Attività di audit e certificazione
- Utilizzo del case study per sviluppare la fase di Formazione e esercitazioni

Sessione 7: Conclusioni e valutazione del corso

- Conclusioni
- Test finale di apprendimento

Nota: questo indice potrebbe variare a seconda delle esigenze e dei requisiti specifici dei partecipanti al corso.

Per i corsi in presenza:

Il corso si terrà di persona e il test finale di apprendimenti si terrà il pomeriggio dell'ultimo giorno. Per questo corso è necessario un computer, connesso a Internet.

Per i corsi tenuti online:

Tutti i corsi online si tengono tramite piattaforma GoToMeeting, Teams o 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 ai materiali del corso prima dell'inizio del corso.

Costo, iscrizione e ulteriori informazioni

Consultare il sito www.continuitaly.it Scrivere a info@continuitaly.it

Corso intensivo sul Crisis Management secondo lo standard ISO22361:2022

Durata: 2 giorni di lezione dalle 9:00 alle 18:00
Esame: test finale di apprendimento a risposta multipla
Incluso nel costo del corso

- Corso online o in presenza erogato in italiano o inglese
- Materiale del corso in italiano o inglese e in formato digitale
- Attestato di partecipazione

Descrizione
ISO 22361:2022 è uno standard internazionale per il crisis management, pubblicato nel gennaio 2022. Lo standard definisce le linee guida per la gestione delle crisi, comprendendo la preparazione, la risposta e la ripresa dalle situazioni di emergenza e di crisi. Il documento è stato creato con l'obiettivo di fornire un approccio sistematico e basato sui rischi per la gestione delle crisi, applicabile a qualsiasi organizzazione, indipendentemente dalla sua dimensione, tipologia o settore di appartenenza. Inoltre, lo standard si concentra sulla necessità di garantire la continuità delle operazioni e la sicurezza delle persone, dei beni e dell'ambiente. Lo standard ISO 22361:2022 si compone di sei parti principali, che descrivono il processo di gestione delle crisi dall'inizio alla fine:

- Ambito di applicazione: definisce i requisiti di base per l'implementazione del sistema di gestione delle crisi, compresi i principi, gli obiettivi e gli scopi dello standard.
- Riferimenti normativi: elenca i documenti di riferimento, compresi gli standard internazionali e le normative locali, che possono essere utilizzati per supportare l'implementazione del sistema di gestione delle crisi.
- Termini e definizioni: definisce i termini chiave utilizzati nello standard per garantire una comprensione comune dei concetti.
- Requisiti del sistema di gestione delle crisi: descrive i requisiti essenziali per l'implementazione del sistema di gestione delle crisi, compresi l'identificazione dei rischi, la pianificazione, la preparazione, la risposta e la ripresa dalle crisi.
- Implementazione del sistema di gestione delle crisi: fornisce una guida pratica per l'implementazione del sistema di gestione delle crisi, compresi i processi di pianificazione, preparazione, risposta e ripresa.
- Monitoraggio, valutazione e miglioramento del sistema di gestione delle crisi: descrive le attività di monitoraggio, valutazione e miglioramento del sistema di gestione delle crisi, compresi il monitoraggio delle prestazioni, la valutazione dei risultati e l'implementazione di azioni correttive.

Lo standard ISO 22361:2022 è stato progettato per essere compatibile con altri standard di gestione, come ISO 9001 (qualità), ISO 14001 (ambiente) e ISO 45001 (sicurezza sul lavoro), consentendo alle organizzazioni di integrare la gestione delle crisi all'interno dei loro sistemi di gestione esistenti. In sintesi, ISO 22361:2022 è uno standard completo e flessibile per la gestione delle crisi, che fornisce una guida pratica per le organizzazioni di ogni dimensione e settore. L'implementazione di questo standard può aiutare le organizzazioni a migliorare la loro capacità di affrontare situazioni di emergenza e di crisi, minimizzando gli

effetti negativi sulle loro attività e sui loro stakeholder.

Struttura del corso
Il corso prevede una combinazione di sessioni teoriche, esercitazioni pratiche, casi studio e discussioni. Gli istruttori dispongono di una solida conoscenza dello standard ISO 22361:2022 e dell'esperienza pratica nella gestione delle crisi, in modo da poter fornire un supporto efficace e personalizzato ai partecipanti del corso.

Primo giorno

Sessione 1: Introduzione allo standard ISO 22361:2022

- Presentazione del corso e degli obiettivi
- Panoramica dello standard ISO 22361:2022
- Principi fondamentali della gestione delle crisi

Sessione 2: Requisiti del sistema di gestione delle crisi

- Identificazione dei rischi e valutazione della vulnerabilità
- Pianificazione della gestione delle crisi
- Preparazione alla gestione delle crisi

Sessione 3: Implementazione del sistema di gestione delle crisi

- Risposta alle emergenze e gestione delle crisi
- Gestione delle informazioni e comunicazione
- Gestione della continuità delle attività

Sessione 4: Esercitazioni e casi studio

- Discussione di casi studio di gestione delle crisi
- Esercitazioni pratiche sulla preparazione, risposta e ripresa dalle crisi

Secondo giorno

Sessione 5: Monitoraggio, valutazione e miglioramento del sistema di gestione delle crisi

- Monitoraggio delle prestazioni del sistema di gestione delle crisi
- Valutazione dei risultati e miglioramento continuo
- Implementazione di azioni correttive

Sessione 6: Integrazione del sistema di gestione delle crisi con altri sistemi di gestione

- Integrazione del sistema di gestione delle crisi con ISO 9001, ISO 14001 e ISO 45001
- Sinergie tra i diversi sistemi di gestione

Sessione 7: Audit e certificazione del sistema di gestione delle crisi

- Audit del sistema di gestione delle crisi
- Certificazione del sistema di gestione delle crisi

Sessione 8: Conclusioni e valutazione del corso

- Sintesi dei contenuti del corso
- Test finale di apprendimento
- Feedback e domande finali

Nota: questo indice potrebbe variare a seconda delle esigenze e dei requisiti specifici dei partecipanti al corso.

Per i corsi in presenza:

Il corso si terrà di persona e il test finale di apprendimenti si terrà il pomeriggio dell'ultimo giorno. Per questo corso è necessario un computer, connesso a Internet.

Per i corsi tenuti online:

Tutti i corsi online si tengono tramite piattaforma GoToMeeting, Teams o 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 ai materiali del corso prima dell'inizio del corso.

Costo, iscrizione e ulteriori informazioni

Consultare il sito www.continuitaly.it Scrivere a info@continuitaly.it

Corso intensivo sul Risk Management secondo lo standard ISO31000

Durata: 2 giorni di lezione dalle 9:00 alle 18:00
Esame: test finale di apprendimento a risposta multipla
Incluso nel costo del corso

- Corso online o in presenza erogato in italiano o inglese
- Materiale del corso in italiano o inglese e in formato digitale
- Attestato di partecipazione

Descrizione
Lo standard ISO 31000 fornisce un quadro per la gestione del rischio, che può essere utilizzato da qualsiasi organizzazione, pubblica o privata, grande o piccola, e in qualsiasi contesto. L'obiettivo principale dello standard è quello di aiutare le organizzazioni a sviluppare un approccio sistematico e coerente alla gestione del rischio, al fine di migliorare la loro capacità di affrontare le sfide e le opportunità che si presentano.
Lo standard ISO 31000 definisce il rischio come "l'effetto dell'incertezza sui risultati previsti". Ciò significa che il rischio si verifica quando c'è incertezza riguardo ai risultati di un'azione o di una decisione. Ad esempio, quando un'azienda decide di espandersi in un nuovo mercato, ci sono sempre rischi associati a questa decisione, come la possibilità di perdere denaro, la mancanza di domanda per i loro prodotti o servizi, ecc. Lo standard prevede un processo di gestione del rischio in cui le organizzazioni devono:

- Stabilire il contesto: comprendere il contesto in cui operano, i loro obiettivi e le esigenze delle parti interessate.
- Identificare il rischio: individuare le fonti di rischio e gli eventi che potrebbero influenzare il raggiungimento degli obiettivi dell'organizzazione.
- Analizzare il rischio: valutare la probabilità e l'impatto dei rischi identificati.
- Valutare il rischio: valutare il rischio complessivo e decidere se accettarlo, mitigarlo o trasferirlo.
- Trattare il rischio: implementare le misure di gestione del rischio per mitigare o eliminare i rischi.
- Monitorare e revisionare: monitorare e controllare il rischio e revisionare il processo di gestione del rischio per migliorare continuamente.
- Lo standard fornisce anche linee guida per la comunicazione e la consultazione con le parti interessate e per l'integrazione della gestione del rischio nell'intera organizzazione.

Ci sono diversi vantaggi nell'adottare lo standard ISO 31000 per la gestione del rischio. In primo luogo, aiuta a migliorare la trasparenza e la responsabilità nella gestione del rischio, garantendo che le decisioni siano prese in modo coerente e basato sui fatti. In secondo luogo, aiuta a ridurre i costi e a migliorare l'efficienza, identificando e gestendo i rischi in modo proattivo e prevenendo i problemi prima che si verifichino. In terzo luogo, aiuta a migliorare la reputazione e la fiducia degli stakeholder, dimostrando che l'organizzazione ha un approccio rigoroso e professionale alla gestione del rischio. L'implementazione dello standard richiede una forte leadership e un impegno a lungo termine da parte dell'organizzazione. Inoltre, l'applicazione del processo di gestione del rischio può essere complessa e richiedere risorse significative. Tuttavia, i vantaggi a lungo termine superano di gran lunga gli investimenti.
Struttura del corso
Il corso di due giorni dedicato allo standard ISO 31000 fornisce una panoramica dettagliata dei principi, dei concetti e delle linee guida per la gestione del rischio. Durante il corso, verranno esaminate le diverse fasi

del processo di gestione del rischio e verranno forniti esempi pratici di come applicare tali principi e linee guida in una varietà di contesti organizzativi. Inoltre, il corso coprirà anche gli aspetti chiave della valutazione del rischio, della gestione del rischio e della comunicazione del rischio.

Giorno 1:

- Introduzione allo standard ISO 31000
- Concetti chiave della gestione del rischio
- Processo di gestione del rischio: identificazione, analisi, valutazione e trattamento del rischio
- Comunicazione del rischio
- Esercizi pratici

Giorno 2:

- Revisione dei principali concetti della giornata precedente
- Valutazione del rischio: analisi qualitativa e quantitativa del rischio
- Gestione del rischio: selezione di opzioni di trattamento del rischio e implementazione di azioni correttive
- Ruolo della leadership nella gestione del rischio
- Esercizi pratici e discussione di casi di studio
- Test finale di apprendimento

Nota: questo indice potrebbe variare a seconda delle esigenze e dei requisiti specifici dei partecipanti al corso.

Per i corsi in presenza:

Il corso si terrà di persona e il test finale di apprendimenti si terrà il pomeriggio dell'ultimo giorno. Per questo corso è necessario un computer, connesso a Internet.

Per i corsi tenuti online:

Tutti i corsi online si tengono tramite piattaforma GoToMeeting, Teams o 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 ai materiali del corso prima dell'inizio del corso.

Costo, iscrizione e ulteriori informazioni

Consultare il sito www.continuitaly.it Scrivere a info@continuitaly.it