

Disaster Recovery Professional (EDRP)

CODICE	DT0109
DURATA	5 gg
PREZZO	3.500,00 €
EXAM	

DESCRIZIONE

L'EC-Council Disaster Recovery Professional (EDRP), aggiornato alla versione 4 è una certificazione di resilienza aziendale di livello manageriale, progettata per fornire ai professionisti le competenze necessarie a guidare, pianificare e gestire le attività di Business Continuity e Disaster Recovery (BCDR) prima, durante e dopo gli incidenti. Supporta le organizzazioni nel prepararsi alle interruzioni, riducendo al minimo l'impatto operativo e finanziario e rafforzando la resilienza complessiva.

Il corso EC-Council Disaster Recovery Professional (EDRP) copre l'intero ciclo di vita della resilienza aziendale, includendo Business Continuity, Disaster Recovery, valutazione dei rischi, Business Impact Analysis (BIA), gestione delle crisi, backup e ripristino, governance, compliance, test e miglioramento continuo.

Esplora inoltre come Artificial Intelligence, ML, Generative AI, AIOps, automazione e tecnologie cloud possano migliorare l'analisi del rischio, la pianificazione della continuità, il processo decisionale e le attività di ripristino.

- AI e Cloud-Ready: applica AI, ML, GenAI, AIOps, automazione e tecnologie emergenti alle moderne strategie di resilienza.
- Standard globali e governance: copre ISO 22301, requisiti normativi, Zero Trust, AI governance e best practice BCDR.
- Resilienza end-to-end: consente ai professionisti di progettare, implementare, testare e migliorare continuamente i programmi BCDR utilizzando metodologie strutturate come PDCA.

TARGET

Questo corso si rivolge ai professionisti IT della continuità e ripresa di attività, ai consulenti di continuità e ripresa di attività, ai consulenti e managers del rischio IT, ai CISO e Direttori IT.

PREREQUISITI

Nessuno

Module 01 Foundations of Business Continuity and Disaster Recovery

- LO#01: Define the fundamental principles, objectives, and terminology to differentiate between business continuity (BC) and disaster recovery (DR).
- LO#02: Identify and describe legal requirements, standards, and regulations that influence BCDR planning and program execution.
- LO#03: Discuss the strategic importance of establishing and coordinating BC and DR programs to increase and enhance operational resilience.
- LO#04: Recognize best practices for implementing BC and DR.
- LO#05: Explain the role of Artificial Intelligence (AI), Machine Learning (ML), Generative AI, and AIOps in modern resilience programs.
- LO#06: Describe how emerging technologies are transforming continuity, recovery, and operational resilience practices.

Module 02 Business Continuity Management

- LO#01: Describe business continuity management (BCM), its purpose, and how AI technologies support organizational resilience and continuity operations.
- LO#02: Identify the core elements of business continuity management to include AI governance and operational resilience considerations.
- LO#03: Describe the business continuity management lifecycle model.
- LO#04: Recognize legal and regulatory requirements related to BCM and AI.
- LO#05: Describe the concept of Zero Trust framework and how it can enhance BCDR planning.
- LO#06: Identify the roles and responsibilities of the team responsible for implementing BCM.
- LO#07: List key BCM documentation.
- LO#08: Discover how to integrate BCM into daily operations and organizational culture.

Module 03 Risk Assessment

- LO#01: Define risk, identify relevant risk categories and discuss IT disaster recovery ITDR and AI-specific risk considerations.
- LO#02: Discuss risk management and explain its role in business continuity management (BCM) and IT DR.
- LO#03: Identify and discuss the steps in the risk assessment lifecycle and identify AI-implications.
- LO#04: Characterize the roles and responsibilities of individuals responsible for the risk assessment process.
- LO#05: Describe the common techniques used for risk identification, identify the importance of risk documentation, and recognize the importance of validation, testing, and continuous improvement.

- LO#06: Understand dependency mapping and cascading risks.
- LO#07: List risk treatment options and discuss risk mitigation approaches for BCM and IT DR.
- LO#08: Describe risk prioritization based on likelihood, impact, and time.

Module 04 Business Impact Analysis

- LO#01: Describe traditional Business Impact Analysis (BIA), identify its scope, assumptions, key considerations, constraints and AI-related contemplations.
- LO#02: Explain how the BIA support the prioritization of critical business functions, processes, and supporting business and IT resources.
- LO#03: Conduct a Business Impact Analysis using qualitative and quantitative evaluation techniques and how AI can enhance the BIA effort.
- LO#04: Analyze, document, and communicate BIA findings, translating business impact requirements into actionable recovery and resilience decisions.

Module 05 Business Continuity Plan

- LO#01: Describe the contents, purpose, and importance of a Business Continuity Plan in mitigating operational disruptions and supporting organizational resilience.
- LO#02: Explain how AI technologies support business continuity planning, resilience monitoring, and decision-making and select appropriate recovery strategies for critical operations, personnel, facilities, and IT systems.
- LO#03: Develop a complete Business Continuity Plan, incorporating incident response, communication, and recovery planning elements and addressing continuity risks associated with AI-dependent business operations and third-party AI services.

Module 06 Disaster Recovery Planning

- LO#01: Review foundational IT disaster recovery planning concepts and its role in business continuity.
- LO#02: Identify key inputs required for IT disaster recovery planning to include AI considerations.
- LO#03: Identify and analyze risks, threats, and data loss scenarios affecting IT infrastructure, applications, and data.
- LO#04: Explain why IT disaster recovery is essential for safeguarding vital data, minimizing operational interruptions, and ensuring ongoing business operations and how AI can support disaster recovery efforts.
- LO#05: Describe common disaster recovery strategies and their role in organizational resilience.

Module 07 Data Backup and System Recovery

- LO#01: Describe the core concepts of data recovery.
- LO#02: Identify and classify types of data recovery and backup models to include AI optimization.
- LO#03: Evaluate data recovery tools, technologies, and architectures to include AI-assisted

approaches.

- LO#04: Describe best practices for implementing and operating data recovery capabilities.

Module 08 Disaster Recovery Plan Development

- LO#01: Describe the purpose and importance of a disaster recovery plan in mitigating the effects of events that impact IT systems.
- LO#02: Identify and describe disaster recovery plan structure, components, and AI enhancements.
- LO#03: Discuss best practices for developing a clear, usable, and adaptable disaster recovery plan that leverages AI elements.

Module 09 Business Continuity and Disaster Recovery Plan Activation

- LO#01: Determine when business continuity and disaster recovery plans should be activated based on conditions, impacts, and predefined activation criteria.
- LO#02: Initiate and manage the activation process for business continuity and disaster recovery plans, including alerting, escalation, and formal declaration procedures.
- LO#03: Coordinate response activities using defined roles, responsibilities, and incident command structures, ensuring effective collaboration across internal teams and external partners.
- LO#04: Manage crisis communications during plan activation, including internal notifications, external stakeholder engagement, and responses to media inquiries.

Module 10 Business Continuity and Disaster Recovery Plan Activation Test, Training, and Exercise

- LO#01: Define and differentiate BCDR testing methods used to evaluate plan effectiveness.
- LO#02: Identify and apply test, training, and exercise types and integrate performance metrics, KPIs, and dashboards.
- LO#03: Explain how audits, testing, and maturity models support continuous improvement.
- LO#04: Justify the necessity of continual testing in dynamic operational and technology environments.