EC-COUNCIL



EC-COUNCIL · PROGRAMA DE RESILIENCIA EMPRESARIAL

EC-Council Disaster Recovery Professional (EDRP) v4

Lidere la recuperación, fortalezca la resiliencia y domine la continuidad del negocio con apoyo de la inteligencia artificial

¿Por qué debería asistir?

El EC-Council Disaster Recovery Professional (EDRP) es una certificación integral de resiliencia empresarial, de nivel gerencial, que prepara a los profesionales para liderar, planificar y gestionar las actividades de continuidad del negocio y recuperación ante desastres (BC/DR) antes, durante y después de un incidente. Cubre el ciclo completo de la resiliencia: riesgos, análisis de impacto al negocio (BIA), gestión de crisis, respaldo y recuperación, activación, pruebas y mejora continua.

Diseñada para entornos impulsados por la nube y la IA, la versión 4 aplica IA, IA generativa, AIOps y automatización al análisis de riesgos y a las decisiones de recuperación, alineada con ISO 22301, los requisitos regulatorios, Zero Trust y el modelo PDCA.

5 días	10	10	12	5
DURACIÓN	MÓDULOS	LABORATORIOS	EJERCICIOS	CASOS DE ESTUDIO



¿Quién debería participar?

Gerentes de TI y de seguridad
Pasar de proteger sistemas a construir organizaciones resilientes, conectando las operaciones de ciberseguridad con la gestión de continuidad y DR.

Gerentes de continuidad y DR
Modernizar la experiencia en BC/DR para entornos en la nube, híbridos y con IA, y fortalecer las pruebas y la mejora continua.

Gerentes de riesgo empresarial
Convertir las evaluaciones de riesgo en prioridades de recuperación, vinculando la gestión de riesgos con el BIA, la BCM y la estrategia de DR.

Respuesta a incidentes y nuevos líderes
Gerentes de respuesta a incidentes y profesionales que aspiran a liderar la resiliencia, incluidos auditores de TI y equipos GRC.

Objetivos de aprendizaje

- Diferenciar los conceptos de continuidad del negocio y recuperación ante desastres, y aplicar los principios de resiliencia organizacional
- Identificar las normas, regulaciones y requisitos legales de BC/DR, y describir el ciclo de vida de la BCM y el modelo PDCA
- Realizar evaluaciones de riesgo y análisis de impacto al negocio, mapeando dependencias y riesgos en cascada
- Establecer objetivos de recuperación (RTO, RPO y MTD) según las necesidades del negocio
- Desarrollar planes de continuidad del negocio y de recuperación ante desastres para sistemas, aplicaciones y datos
- Evaluar estrategias de recuperación en la nube, híbridas y automatizadas, e implementar estrategias modernas de respaldo
- Activar los planes BC/DR con escalamiento, coordinación y comunicación de crisis estructurados
- Medir y mejorar la resiliencia mediante pruebas, ejercicios, KPIs, auditorías y herramientas de IA y AIOps

Áreas de habilidad del programa

Resiliencia organizacional integral | Planificación del riesgo a la recuperación | DR moderno en la nube e híbrido | Pruebas por escenarios y mejora continua | Gestión de crisis y liderazgo | BC/DR impulsado por IA | ISO 22301 y PDCA

Programa del curso

Duración: 5 días

Módulo	Contenido
Módulos 1–2 Día 1	**01 Fundamentos de continuidad del negocio y recuperación ante desastres:** resiliencia organizacional, BC vs. DR, evolución, normas y regulaciones, mejores prácticas, IA, ML, IA generativa, AIOps y tecnologías emergentes. Cinco casos de estudio: Target, Maersk/NotPetya, Southwest Airlines, TSMC y Toyota. **02 Gestión de la continuidad del negocio:** ciclo de vida de la BCM, BIA, evaluación de riesgos, modelado de amenazas, estrategias de continuidad, gestión y comunicación de crisis, pruebas y ejercicios, ISO 22301, gobierno de IA y Zero Trust.
Módulos 3–4 Día 2	**03 Evaluación de riesgos:** ciclo de evaluación, identificación, análisis, evaluación y tratamiento de riesgos, registro y matriz de riesgos, mapeo de dependencias, riesgos en cascada y de terceros, riesgos de IA. Laboratorio: evaluación cualitativa con MONARC. **04 Análisis de impacto al negocio:** BIA potenciado con IA, funciones y procesos críticos, dependencias de negocio, TI y terceros, niveles mínimos de servicio, análisis de impacto en el tiempo, RTO y RPO, recolección y reporte del BIA.
Módulos 5–6 Día 3	**05 Plan de continuidad del negocio:** estructura del BCP, BCP vs. DRP, estrategias de continuidad para personal, instalaciones, TI y datos, continuidad con IA, respaldo y anulación manual de IA, respuesta a incidentes y comunicación de crisis. **06 Planificación de la recuperación ante desastres:** recuperación de infraestructura, aplicaciones y datos, estrategias de DR, orquestación automatizada, DR en la nube, DRaaS, recuperación en clean room, retención de datos e infraestructura autorreparable.
Módulos 7–8 Día 4	**07 Respaldo de datos y recuperación de sistemas:** respaldos completos, incrementales y diferenciales, CDP, respaldos inmutables, recuperación ante ransomware, VM, Kubernetes y Docker. Nueve laboratorios: Shadow Copy, BorgBackup, Windows Server Backup, Hyper-V y más. **08 Desarrollo del plan de recuperación ante desastres:** propósito y estructura del DRP, escenarios de disrupción, roles y responsabilidades, recursos, proveedores y procedimientos, flujos y runbooks generados con IA, y mantenimiento del plan.
Módulos 9–10 Día 5	**09 Activación de los planes de continuidad y recuperación:** criterios y disparadores de activación, escalamiento, declaración de desastre, estructura de comando del incidente, coordinación con partes externas, comunicación de crisis, medios y desinformación. **10 Pruebas, capacitación y ejercicios de activación de los planes BC/DR:** planificación y ejecución de pruebas, escenarios generados con IA, KPIs y tableros, gemelos digitales, auditorías, modelos de madurez, lecciones aprendidas y mejora continua.



Examen

Duración: 4 horas

Título	EC-Council Disaster Recovery Professional (EDRP) – Versión 4		
Código	312-76	**N.º de preguntas**	150
Formato	Opción múltiple	**Duración**	4 horas
Aprobación	70 %	**Plataforma**	ECC Exam Portal

Requisitos y experiencia recomendada

- **Sin prerrequisito obligatorio:** el programa está abierto a profesionales que desean pasar de roles técnicos u operativos al liderazgo estratégico de la resiliencia.
- **Experiencia recomendada:** de 2 a 4 años en administración de infraestructura de TI, operaciones de seguridad de redes, gestión de riesgos, respuesta a incidentes o campos relacionados.

Roles profesionales asociados a EDRP

Gerente de BC/DR, oficial de continuidad del negocio, gerente de resiliencia operacional, gerente de recuperación ante desastres de TI, gerente de riesgos de TI, gerente de respuesta a incidentes, oficial de gestión de crisis y consultor de BC/DR o de resiliencia de TI.

Información general

- Un año de acceso al material digital y a los videos de capacitación, y seis meses de acceso a los laboratorios
- Voucher de examen supervisado con validez de un año
- Credencial acreditada por ANAB (ISO/IEC 17024) y reconocida por el DoD 8570/8140

