

Programa da ação

Continuidade de Negócio, Cópias de Segurança e Recuperação de Desastres

Percurso formativo em Cibersegurança — Ação 4 de 6 (sequência cumulativa de 300 horas).

Identificação	Caracterização
Área temática	Tecnologias de Informação e Comunicação / Resiliência e Recuperação
Duração total	50 horas
Modalidade	100% aulas síncronas online através do Microsoft Teams
Nível	Formação técnica de iniciação, com progressão prática supervisionada
Público-alvo	Adolescentes, jovens e adultos em iniciação técnica à cibersegurança, conforme as condições de acesso da candidatura.
Pré-requisitos	Acções 1 a 3 concluídas ou conhecimento equivalente de ativos, serviços e dependências.

Descrição da formação

Esta ação desenvolve competências práticas para reduzir a perda de dados e a indisponibilidade de serviços. Os participantes configuram backups e testam restauros, estabelecem objectivos de recuperação, efectuem uma análise de impacto no negócio (BIA) simplificada e preparam versões introdutórias de um plano de continuidade de negócio (PCN) e de um plano de recuperação de desastres (DRP).

Enquadramento e articulação no percurso de 300 horas

Quarta ação. Recebe da ação 1 os ativos críticos, da ação 2 o mapa técnico e da ação 3 as dependências externas. Ao contrário da primeira ação, o foco é a execução de backups, a medição de restauros e a organização da continuidade perante interrupções reais ou simuladas.

Objetivo geral

Capacitar os participantes para seleccionar e verificar estratégias elementares de backup, estabelecer prioridades de continuidade, produzir um PCN e um DRP introdutórios e testar ambos em cenários controlados.

Objetivos específicos

No final da ação, cada formando deverá ser capaz de:

- Distinguir tipos de cópia de segurança, retenção, protecção contra ransomware e restauro.
- Executar e verificar uma cópia de segurança de ficheiros em ambiente de treino.
- Interpretar RPO e RTO e distingui-los de resultados reais observados.

- Identificar processos críticos e dependências com uma BIA simplificada.
- Preparar estratégias alternativas de funcionamento e comunicação de crise.
- Construir um PCN introdutório com critérios de activação e responsáveis.
- Definir sequência de recuperação, dependências técnicas e testes num DRP.
- Conduzir exercício de mesa e documentar resultados e melhorias.

Metodologia

A ação decorre integralmente em 20 sessões síncronas de 2 horas e 30 minutos, em Microsoft Teams. Cada um dos 10 módulos corresponde a 5 horas: 2 horas de explicação e demonstração e 3 horas de prática orientada e avaliação. Deste modo, as 50 horas incluem todos os exercícios, oficinas, apresentações, revisão e avaliação. Não existem horas assíncronas, trabalhos obrigatórios fora das sessões nem formação em contexto de trabalho (FCT).

O formador apresenta os conceitos de forma gradual, demonstra os procedimentos e acompanha tarefas individuais e em grupo. A execução utiliza uma organização fictícia comum às seis ações, designada Atlântico Serviços (nome fictício), com cerca de 30 trabalhadores, portal de clientes, ficheiros administrativos, serviços cloud, rede interna e fornecedores externos. Os dados, contas e registos são simulados; os laboratórios técnicos são isolados ou expressamente autorizados. Cada etapa produz evidências documentadas, e a sua avaliação individual não depende da dimensão do grupo.

As primeiras sessões começam com diagnóstico de competências sem classificação. O formador disponibiliza glossário, instruções, modelos e critérios antes das atividades. A complexidade aumenta através da aplicação dos conhecimentos anteriores a situações novas; quando um conceito transversal reaparece, é mobilizado como pré-requisito, sem nova aula de fundamentos.

Plano de aulas

Mód.	Aulas	Tema	Explic.	Prática	Total
M1	1 e 2	Fundamentos de cópias de segurança e restauro	2 h	3 h	5 h
M2	3 e 4	Execução e protecção de backups	2 h	3 h	5 h
M3	5 e 6	Restauro testado e medição de resultados	2 h	3 h	5 h
M4	7 e 8	Continuidade de negócio e análise de impacto	2 h	3 h	5 h
M5	9 e 10	Estratégias e plano de continuidade de negócio	2 h	3 h	5 h
M6	11 e 12	Exercícios e melhoria da continuidade	2 h	3 h	5 h
M7	13 e 14	Recuperação de desastres e DRP	2 h	3 h	5 h
M8	15 e 16	Oficina: política de backup e execução de restauro	2 h	3 h	5 h
M9	17 e 18	Oficina: BIA e PCN com dependências externas	2 h	3 h	5 h
M10	19 e 20	Projeto integrador: DRP e simulação final	2 h	3 h	5 h
Total	20 sessões	10 módulos	20 h	30 h	50 h

Distribuição de horas por modalidade

Modalidade	Horas	Percentagem
Aulas síncronas online no Microsoft Teams	50 h	100%
Total	50 h	100%

A distribuição entre explicação, demonstração, prática e avaliação representa actividades pedagógicas na mesma modalidade síncrona.

Conteúdos programáticos

M1 — Fundamentos de cópias de segurança e restauro (5 horas)

- Perda, corrupção, eliminação acidental, ransomware e indisponibilidade.
- Backup completo, incremental e diferencial; vantagens e limitações.
- Regra 3-2-1, cópia offline, retenção e protecção do armazenamento.
- Introdução a RPO e RTO com exemplos de processos da empresa fictícia.

Atividade prática: Seleccionar estratégia de backup e justificar periodicidade e retenção.

Evidência de aprendizagem: Quadro de selecção com RPO e RTO pretendidos.

M2 — Execução e protecção de backups (5 horas)

- Definição de origem, destino, agendamento e permissões de cópia.
- Cifragem, controlo de acesso, protecção offline e imutabilidade como opções.
- Verificação de execução e leitura de relatórios de erros.
- Separação entre backup criado e restauro efectivamente testado.

Atividade prática: Configurar cópia de ficheiros fictícios e confirmar integridade do conjunto.

Evidência de aprendizagem: Relatório de execução, falhas corrigidas e evidências de backup.

M3 — Restauro testado e medição de resultados (5 horas)

- Restauro de ficheiro e de conjunto de dados em ambiente isolado.
- Sequência de recuperação, dependências, versão e permissões.
- Medição de tempo de restauro e verificação da informação recuperada.
- Comparação entre resultado observado, RTO e RPO definidos.

Atividade prática: Restaurar um conjunto de teste e medir o resultado.

Evidência de aprendizagem: Registo de restauro com tempos, verificação e conclusão.

M4 — Continuidade de negócio e análise de impacto (5 horas)

- Continuidade operacional versus restauro técnico de sistemas.
- Processos essenciais e consequências de interrupções.
- BIA simplificada: recursos, dependências, impacto por duração e prioridades.
- Documentação da tolerância a interrupções no contexto simulado.

Atividade prática: Construir BIA de três processos com base nos dados do caso.

Evidência de aprendizagem: Tabela BIA com prioridades, dependências e impactos.

M5 — Estratégias e plano de continuidade de negócio (5 horas)

- Soluções alternativas de pessoas, locais, fornecedores e comunicações.
- Critérios de activação e decisão de continuidade.
- Estrutura do PCN: objectivo, âmbito, equipa, contactos e medidas.
- Registo de alterações e revisão após exercícios e mudanças.

Atividade prática: Redigir plano de continuidade para um processo crítico.

Evidência de aprendizagem: Primeira versão do PCN com contactos fictícios e critérios de activação.

M6 — Exercícios e melhoria da continuidade (5 horas)

- Revisão documental, exercício de mesa e simulação: diferenças.
- Preparação de cenário, papéis, instruções e critérios de sucesso.
- Registo de decisões, tempos e obstáculos verificados.
- Plano de melhoria e atribuição de responsáveis.

Atividade prática: Realizar exercício de mesa sobre indisponibilidade de local ou fornecedor.

Evidência de aprendizagem: Acta de exercício, incidentes simulados e acções de melhoria.

M7 — Recuperação de desastres e DRP (5 horas)

- Diferença entre PCN e DRP e relação entre negócios e sistemas.
- Dependências de aplicação, servidores, rede, dados e fornecedores.
- Estratégias de reposição, restauração e funcionamento alternativo.
- Estrutura de DRP, responsáveis e pré-condições para activar recuperação.

Atividade prática: Ordenar a recuperação de três serviços segundo as suas dependências.

Evidência de aprendizagem: Esquema de precedências e esboço do DRP.

M8 — Oficina: política de backup e execução de restauro (5 horas)

- Consolidação de catálogo de dados e destinos de cópia.

- Ajustamento dos calendários de retenção à necessidade do serviço.
- Teste supervisionado de restauro com verificação de ficheiros.
- Actualização de procedimento e instruções de execução.

Atividade prática: Concluir política simplificada e repetir restauro após uma falha introduzida.

Evidência de aprendizagem: Política de backup e segundo registo de restauro.

M9 — Oficina: BIA e PCN com dependências externas (5 horas)

- Conferência dos processos, prioridades e dependências documentadas.
- Incorporação dos fornecedores críticos da ação 3.
- Determinação de alternativas operacionais e responsáveis.
- Revisão de coerência entre BIA e medidas previstas no PCN.

Atividade prática: Rever BIA e concluir PCN para interrupção prolongada de fornecedor.

Evidência de aprendizagem: BIA e PCN revistos, acompanhados de checklist de activação.

M10 — Projeto integrador: DRP e simulação final (5 horas)

- Integração de backups, BIA, PCN e DRP.
- Exercício de mesa com interrupção simultânea de serviço e perda de dados.
- Documentação de decisões, tempos estimados e resultados de testes.
- Comunicação final de lições aprendidas e plano de melhoria.

Atividade prática: Simular recuperação de serviço da empresa fictícia e defender decisões.

Evidência de aprendizagem: Dossier de backup, evidências de restauro, BIA, PCN, DRP e relatório de teste.

Projeto integrador e avaliação final

O módulo 10 encerra e avalia a ação, sem horas adicionais. O projecto desenvolve-se progressivamente durante as sessões e culmina numa entrega individual, ainda que a elaboração de partes do exercício possa envolver colaboração entre pares. O formador observa tarefas executadas, confirma a autoria individual e verifica as evidências propostas.

Produto final da ação: Política e evidências de backup e restauro; BIA simplificada, PCN, DRP e acta de exercício de continuidade.

Modalidades e ponderações da avaliação

Componente	Instrumento	Peso
Diagnóstica	Questionário inicial e apoio às dificuldades	Sem peso
Formativa	Questionários curtos e verificação de compreensão	20%

Formativa	Tarefas práticas individuais realizadas em aula	20%
Sumativa	Projeto integrador e demonstração individual	60%
Total		100%

Critérios de classificação do projeto

Critério	Peso no projeto (%)
Configuração de backups e evidências de restauro	25%
Qualidade da BIA e prioridades de continuidade	20%
Exequibilidade e clareza do PCN	20%
Sequência e documentação do DRP	20%
Teste final, lições e comunicação	15%
Total	100%

A classificação final resulta de 20% da nota dos questionários, 20% da nota das tarefas práticas e 60% da nota do projecto. A escala de classificação é de 0 a 20 valores. A aprovação pedagógica requer classificação final igual ou superior a 10 valores e classificação do projecto igual ou superior a 10 valores. Os requisitos administrativos de assiduidade e certificação dependem do regulamento aplicável da entidade formadora.

Continuidade pedagógica e produto para a ação seguinte

A documentação sobre recuperação e fornecedores servirá de contexto aos tratamentos de dados pessoais e, na ação 6, aos cenários de indisponibilidade ou perda de dados. Não substitui os deveres legais de notificação do RGPD.

Recursos e materiais

- Pastas e ficheiros fictícios; espaço de armazenamento controlado; software de cópia adequado ao ambiente de formação.
- Modelos de BIA, PCN e DRP; cronómetros e fichas de resultados.
- Cenários de indisponibilidade, dependências da organização simulada e sala Teams.

A participação deve ser possível com computador, ligação estável à Internet, navegador e Microsoft Teams. Sempre que a instalação de ferramentas não seja viável, o formador utiliza laboratório remoto de treino, partilha de ecrã e ficheiros simulados, assegurando a prática síncrona de todos os formandos.

Modelos de documentação

- Política de backup: origem, destino, método, frequência, retenção, responsável e verificação.
- BIA: processo, dependências, impacto temporal, RTO/RPO desejados e prioridade.

- PCN/DRP: ativação, papéis, contacto, sequência, testes, resultados e melhoria.

Referências técnicas e normativas

International Organization for Standardization. (2019). ISO 22301:2019: Security and resilience — Business continuity management systems — Requirements.
<https://www.iso.org/standard/75106.html>

National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST CSWP 29). <https://doi.org/10.6028/NIST.CSWP.29>

National Institute of Standards and Technology. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST SP 800-61 Rev. 3). <https://doi.org/10.6028/NIST.SP.800-61r3>

Nota: os referenciais são utilizados para enquadramento pedagógico e não equivalem à certificação dos formandos ou à implementação integral de um sistema de gestão.