

Objetivos específicos

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

- Distinguir ativos, ameaças, vulnerabilidades, incidentes, controlos e riscos com exemplos de confidencialidade, integridade e disponibilidade.
- Inventariar equipamentos, aplicações, serviços, documentos, contas e dependências, atribuindo identificadores e responsáveis.
- Classificar informação e justificar a criticidade dos ativos perante falhas de segurança.
- Descrever cenários de risco que indiquem causa, vulnerabilidade, consequência e controlos existentes.
- Aplicar critérios de probabilidade e impacto previamente definidos numa matriz qualitativa de 3×3 .
- Seleccionar prioridades, opções de tratamento, responsáveis, prazos e evidências esperadas.
- Distinguir risco inerente, actual e residual, bem como decisão de aceitação e estimativa não verificada.
- Actualizar e comunicar o estado dos riscos através de um relatório conciso.

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.	Práctica	Total
------	-------	------	---------	----------	-------

M1	1 e 2	Fundamentos de segurança da informação e contexto do risco	2 h	3 h	5 h
M2	3 e 4	Identificação e inventário de ativos	2 h	3 h	5 h
M3	5 e 6	Classificação da informação e criticidade	2 h	3 h	5 h
M4	7 e 8	Ciclo de vida, posse e responsabilidades	2 h	3 h	5 h
M5	9 e 10	Ameaças, vulnerabilidades e cenários de risco	2 h	3 h	5 h
M6	11 e 12	Análise qualitativa e prioridades	2 h	3 h	5 h
M7	13 e 14	Opções de tratamento e selecção de controlos	2 h	3 h	5 h
M8	15 e 16	Plano de tratamento e risco residual	2 h	3 h	5 h
M9	17 e 18	Monitorização e comunicação dos riscos	2 h	3 h	5 h
M10	19 e 20	Oficina integradora: dossier de ativos e riscos	2 h	3 h	5 h
Total	20 aulas	10 módulos	20 h	30 h	50 h

Distribuição de horas por modalidade

Modalidade	Horas	Porcentagem
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 segurança da informação e contexto do risco (5 horas)

- Confidencialidade, integridade e disponibilidade; diferenças entre segurança da informação e cibersegurança.
- Ativo, ameaça, vulnerabilidade, controlo, incidente e risco; exemplos distinguíveis.
- Objectivos da organização, âmbito, intervenientes e funções de governação.
- Visão introdutória da ISO/IEC 27001 e das funções do NIST CSF 2.0.

Atividade prática: Interpretar acontecimentos de uma empresa fictícia e estabelecer o âmbito da análise.

Evidência de aprendizagem: Ficha de contexto e classificação justificada dos conceitos.

M2 — Identificação e inventário de ativos (5 horas)

- Categorias de ativos: informação, hardware, software, contas, serviços e componentes externos.

- Campos essenciais: código, descrição, localização, proprietário, estado e serviço suportado.
- Fontes de levantamento e controlo de qualidade: omissões, duplicados e desactualizações.
- Dependências entre os ativos, os processos e os fornecedores.

Atividade prática: Construir o inventário inicial a partir de fichas de ativos do caso transversal.

Evidência de aprendizagem: Inventário com, pelo menos, 12 ativos identificados e responsáveis atribuídos.

M3 — Classificação da informação e criticidade (5 horas)

- Categorias de sensibilidade e regras de manuseamento definidas no caso de estudo.
- Impacto de perda de confidencialidade, integridade e disponibilidade.
- Criticidade do serviço versus valor de aquisição do equipamento.
- Responsáveis por classificação e revisão periódica.

Atividade prática: Classificar documentos simulados e acrescentar criticidade ao inventário.

Evidência de aprendizagem: Inventário revisto com classificações fundamentadas e medidas de manuseamento propostas.

M4 — Ciclo de vida, posse e responsabilidades (5 horas)

- Aquisição, utilização, manutenção, transferência e retirada de ativos.
- Proprietário do ativo, responsável técnico e utilizador; separação de responsabilidades.
- Entrada e saída de colaboradores como eventos que exigem revisão documental.
- Retirada de serviço, devolução de equipamentos e necessidade de eliminação segura.

Atividade prática: Simular substituição de computador e desactivação de uma conta, actualizando os registos.

Evidência de aprendizagem: Lista de verificação de ciclo de vida e inventário actualizado.

M5 — Ameaças, vulnerabilidades e cenários de risco (5 horas)

- Ameaças humanas, acidentais, ambientais e tecnológicas.
- Vulnerabilidade técnica, organizativa ou física; distinção entre falha real e hipótese.
- Identificação de controlos existentes a partir de evidências fornecidas.
- Formulação de cenários: acontecimento, ativo, fragilidade e consequência.

Atividade prática: Descrever oito cenários concretos que afectem ativos inventariados.

Evidência de aprendizagem: Registo inicial de oito riscos sem duplicações conceptuais.

M6 — Análise qualitativa e prioridades (5 horas)

- Escalas explícitas de probabilidade e impacto de três níveis.

- Matriz 3 × 3 como convenção pedagógica, sem pretensão de fórmula normativa universal.
- Risco inerente e actual; documentação de pressupostos e incerteza.
- Comparação com critérios de aceitação e selecção de prioridades.

Atividade prática: Avaliar os oito cenários e identificar os três mais relevantes.

Evidência de aprendizagem: Matriz coerente, registo de riscos e fundamentação das prioridades.

M7 — Opções de tratamento e selecção de controlos (5 horas)

- Evitar, reduzir, partilhar e aceitar: diferenças entre opções e responsabilidades.
- Controlos preventivos, de detecção e correctivos; medidas humanas, físicas e técnicas.
- Exemplos de controlo: MFA, actualizações, backups, formação e protecção física.
- Correspondência entre cenário, controlo seleccionado e resultado esperado.

Atividade prática: Escolher medidas para os três riscos prioritários, sem as configurar tecnicamente.

Evidência de aprendizagem: Mapa de controlos recomendados com justificações e prioridades.

M8 — Plano de tratamento e risco residual (5 horas)

- Estrutura de plano: risco, acção, responsável, recursos, prazo, estado e evidência.
- Distinção entre medida proposta, aplicada e verificada.
- Estimativa do risco residual e documentação de pressupostos.
- Autoridade competente para aceitar riscos e condições de revisão.

Atividade prática: Elaborar plano com três acções e documentar uma decisão simulada de aceitação.

Evidência de aprendizagem: Plano de tratamento, estimativas residuais e registo de decisão.

M9 — Monitorização e comunicação dos riscos (5 horas)

- Factores que exigem revisão: mudanças técnicas, fornecedores, pessoal e incidentes.
- Indicadores simples: ativos com dono e acções de tratamento concluídas.
- Histórico de versões, evidências e responsáveis pela monitorização.
- Síntese de prioridades para público técnico e não técnico.

Atividade prática: Introduzir uma alteração no cenário e escrever uma comunicação de uma página.

Evidência de aprendizagem: Registo de risco actualizado, indicadores e relatório executivo.

M10 — Oficina integradora: dossier de ativos e riscos (5 horas)

- Validação cruzada de inventário, classificação, cenários e tratamento.
- Verificação da rastreabilidade entre prioridades e medidas.
- Revisão de pressupostos, lacunas documentais e decisões pendentes.
- Apresentação individual de resultados e defesa das opções escolhidas.

Atividade prática: Concluir e apresentar o dossier de segurança da informação da organização fictícia.

Evidência de aprendizagem: Inventário (≥12 ativos), oito cenários avaliados, três ações e relatório executivo final.

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: Inventário de ativos, classificação da informação, registo de riscos, matriz qualitativa e plano de tratamento, com relatório executivo.

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 (%)
Exactidão e rastreabilidade do inventário	20%
Classificação e responsabilidades	15%
Qualidade dos cenários e análise dos riscos	25%
Adequação do plano de tratamento	25%
Comunicação e revisão dos registos	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

O inventário e os riscos prioritários são entregues à ação 2 para análise técnica de rede e sistemas. Na ação 3, as prioridades apoiarão a escolha dos controlos de acesso e a análise das dependências de fornecedores.

Recursos e materiais

- Modelo de inventário, critérios de classificação, matriz 3 × 3 e registo de riscos.
- Fichas da organização fictícia, Excel ou LibreOffice Calc e editor de texto.
- Casos curtos, glossário de segurança, diapositivos e listas de verificação.

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

- Inventário: ID, ativo, tipo, serviço, responsável, localização, estado, criticidade e data de revisão.
- Registo de riscos: cenário, ativo, ameaça, vulnerabilidade, controlos, probabilidade, impacto, prioridade e pressupostos.
- Plano: risco, opção, ação, responsável, prazo, estado, evidência e estimativa residual.

Referências técnicas e normativas

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>

International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. <https://www.iso.org/standard/27001>

International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27005:2022: Information security, cybersecurity and privacy protection — Guidance on managing information security risks. <https://www.iso.org/>

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