

Programa da ação

Controlo de Acesso, Gestão de Identidades e Segurança de Fornecedores

Percurso formativo em Cibersegurança — Ação 3 de 6 (sequência cumulativa de 300 horas).

Identificação	Caracterização
Área temática	Tecnologias de Informação e Comunicação / Controlo de Acesso e Terceiros
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 e 2 concluídas ou competências equivalentes; dispensa experiência profissional em contratação ou procurement.

Descrição da formação

Esta ação desenvolve competências para proteger o acesso a contas, serviços e informação e para acompanhar os riscos decorrentes de prestadores externos. Os formandos configuram gestores de palavras-passe e autenticação multifator em contas de treino, estabelecem perfis de acesso, simulam o ciclo de vida de utilizadores e avaliam fornecedores através de evidências, questionários e requisitos contratuais simples.

Enquadramento e articulação no percurso de 300 horas

Terceira ação. Utiliza o inventário da ação 1 e os serviços identificados na ação 2. A análise de fornecedores considera apenas medidas relativas ao seu acesso, dependências e obrigações de segurança; não substitui o processo global de avaliação de riscos aprendido na ação 1.

Objetivo geral

Capacitar os participantes para propor e aplicar controlos básicos de identidade e acesso e para avaliar a segurança de fornecedores críticos, documentando critérios, evidências e decisões proporcionais.

Objetivos específicos

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

- Reconhecer ameaças a credenciais, phishing e reutilização de palavras-passe.
- Utilizar gestores de palavras-passe e configurar MFA em contas laboratoriais.

- Distinguir autenticação, autorização, privilégios e perfis de acesso.
- Documentar concessão, revisão e revogação de acessos num ciclo de vida simulado.
- Reconhecer requisitos de segurança aplicáveis a prestadores e serviços cloud.
- Preparar e interpretar um questionário introdutório de avaliação de fornecedores.
- Identificar cláusulas de acesso, confidencialidade, notificação de incidentes e continuidade.
- Construir um plano de acompanhamento das dependências e apresentar decisões.

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
M2	3 e 4	Gestores de palavras-passe e MFA	2 h	3 h
M4	7 e 8	Ciclo de vida de identidades e resposta inicial	2 h	3 h
M6	11 e 12	Avaliação e qualificação de fornecedores	2 h	3 h
M8	15 e 16	Monitorização de fornecedores e ocorrências	2 h	3 h
M10	19 e 20	Projeto integrador: políticas e controlo de terceiros	2 h	3 h

Distribuição de horas por modalidade

Modalidade	Horas	Percentagem
------------	-------	-------------

- Contas sem uso, acessos órfãos e desvios face à matriz.
- Medidas imediatas em compromisso suspeito de credenciais; reporte.

Atividade prática: Simular entrada e saída de trabalhador e bloqueio de conta comprometida.

Evidência de aprendizagem: Fluxo de aprovações e registo de revogação e comunicação.

M5 — Fornecedores, dependências e cadeia de abastecimento (5 horas)

- Fornecedores de cloud, suporte, software, alojamento e tratamento de dados.
- Acesso remoto, subcontratação e dependências críticas.
- Noções de ataques à cadeia de abastecimento e exposição de terceiros.
- Inventário de fornecedores construído com base nos serviços já identificados.

Atividade prática: Mapear os acessos e dependências de quatro fornecedores fictícios.

Evidência de aprendizagem: Mapa de dependências com tipo de acesso e importância operacional.

M6 — Avaliação e qualificação de fornecedores (5 horas)

- Questionário baseado em evidências: controlo de acesso, incidentes e continuidade.
- Selecção de requisitos proporcionais ao serviço contratado.
- Interpretação de respostas incompletas, ausência de provas e planos de acção.
- Due diligence introdutória e critérios de aceitação organizacional.

Atividade prática: Aplicar questionário e comparar dois fornecedores fictícios.

Evidência de aprendizagem: Ficha de qualificação com lacunas e recomendações.

M7 — Segurança contratual e responsabilidades (5 horas)

- Cláusulas sobre confidencialidade, níveis de acesso e subcontratação.
- Prazos e canais contratuais de reporte de incidentes; diferenças face ao RGPD.
- Tratamento de dados por terceiros e necessidade de articular responsabilidades.
- Direito de revisão, devolução de dados e saída do fornecedor.

Atividade prática: Rever excertos contratuais simulados e propor requisitos em linguagem clara.

Evidência de aprendizagem: Lista de requisitos de segurança e comentários de revisão contratual.

M8 — Monitorização de fornecedores e ocorrências (5 horas)

- Evidências periódicas, indicadores e registo de compromissos.
- Acompanhamento de não conformidades e planos de correcção.
- Coordenação inicial de ocorrência que afecte um prestador externo.
- Comunicação entre responsável interno, equipa técnica e prestador.

Atividade prática: Simular falha no fornecedor de cloud e preparar pedido formal de esclarecimentos.

Evidência de aprendizagem: Plano de acompanhamento e minuta de comunicação ao prestador.

M9 — Oficina: revisão de acessos e avaliação de terceiros (5 horas)

- Testes supervisionados da matriz de perfis e das configurações de MFA.
- Detecção de excesso de privilégios e contas inativas em dados fictícios.
- Classificação dos fornecedores por dependência e exposição.
- Actualização das recomendações técnicas e documentais.

Atividade prática: Executar revisão cruzada de acessos e completar avaliação de dois prestadores.

Evidência de aprendizagem: Relatório de revisão de acessos e matriz comparativa de fornecedores.

M10 — Projeto integrador: políticas e controlo de terceiros (5 horas)

- Consolidação da política de identidade e das verificações de MFA.
- Integração de requisitos contratuais, mapas de dependências e monitorização.
- Justificação de medidas de privilégio mínimo e resposta a comprometimento.
- Apresentação individual com demonstração de verificações em ambiente de treino.

Atividade prática: Entregar e defender dossier de política de acesso e segurança dos fornecedores.

Evidência de aprendizagem: Matriz de acessos, procedimento de ciclo de vida, checklist MFA e avaliação de terceiros.

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: Matriz de perfis e acessos, política de credenciais e MFA, processo de gestão de identidades e dossier de avaliação de fornecedores.

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 (%)
Qualidade da matriz e do ciclo de vida de acessos	25%
Verificação de credenciais e MFA	20%
Avaliação documentada de fornecedores	25%
Requisitos contratuais e monitorização	20%
Comunicação e defesa individual	10%
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 lista de fornecedores críticos, dependências técnicas e acessos externos é utilizada na ação 4 para identificar processos essenciais, alternativas operacionais e recuperação de serviços.

Recursos e materiais

- Contas de treino, gestor de palavras-passe e mecanismos de MFA disponíveis no laboratório.
- Questionários fictícios de fornecedores, exemplos de contratos, matriz de perfis e fichas de verificação.
- Microsoft Teams, editor de texto, folha de cálculo e cenários simulados.

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

- Matriz de acesso: função, serviço, perfil, permissão, aprovador e data de revisão.
- Avaliação de fornecedor: serviço, dependência, requisitos, evidência, lacuna, acção e responsável.
- Política: critérios de acesso, concessão, revisão, revogação, MFA e reporte.

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>

National Institute of Standards and Technology. (2024). Cybersecurity supply chain risk management practices for systems and organizations (NIST SP 800-161 Rev. 1, Update 1). <https://doi.org/10.6028/NIST.SP.800-161r1-upd1>

Center for Internet Security. (2024). CIS Critical Security Controls (Version 8.1). <https://www.cisecurity.org/controls/v8-1>

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>

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