

Programa da ação

RGPD: Gestão de Violações de Dados Pessoais e Avaliação de Impacto (AIPD)

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

Identificação	Caracterização
Área temática	Proteção de Dados Pessoais / Incidentes e Avaliação de Impacto
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	Ações 1 a 5 concluídas, incluindo RAT da ação 5, ou competências equivalentes; formação especializada complementar poderá ser necessária no exercício profissional.

Descrição da formação

Esta ação aprofunda a resposta a violações de dados pessoais e a avaliação de impacto sobre a protecção de dados (AIPD). Os participantes utilizam o RAT preparado na ação 5 para identificar tratamentos potencialmente sujeitos a AIPD, avaliam consequências para os direitos e liberdades das pessoas, simulam decisões de notificação à CNPD e comunicação aos titulares e elaboram uma AIPD introdutória. Os exercícios seguem critérios documentados, com reconhecimento dos limites da competência técnica inicial.

Enquadramento e articulação no percurso de 300 horas

Sexta e última ação. Usa os documentos produzidos nas cinco ações anteriores, sobretudo o RAT da ação 5, sem reconstruir inventários ou repetir a matriz organizacional de riscos. O risco para os direitos e liberdades dos titulares é tratado de forma própria, distinta do risco de segurança da informação da ação 1.

Objetivo geral

Capacitar os formandos para classificar violações de dados pessoais, fundamentar decisões iniciais de notificação e comunicação e elaborar uma AIPD introdutória com medidas de mitigação e registo de conclusões.

Objetivos específicos

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

- Distinguir incidentes gerais de segurança de violações de dados pessoais, incluindo os efeitos sobre os titulares.
- Registrar factos conhecidos, data de conhecimento, categorias afectadas e acções realizadas.
- Avaliar os limiares legais para notificação à CNPD e comunicação aos titulares.
- Preparar minutas de notificação e comunicação, incluindo o prazo do artigo 33.º e as respectivas condições.
- Distinguir operações do RAT susceptíveis de risco elevado e fundamentar a necessidade de AIPD.
- Descrever finalidade, necessidade e proporcionalidade de um tratamento na AIPD.
- Avaliar riscos específicos para os titulares e propor medidas mitigadoras verificáveis.
- Apresentar dossier final integrado de violação e AIPD, incluindo decisões, incertezas e recomendações.

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	Deteção e caracterização de violações de dados	2 h	3 h	5 h

M2	3 e 4	Risco para os titulares e decisão de notificação	2 h	3 h	5 h
M3	5 e 6	Comunicação a titulares e documentação	2 h	3 h	5 h
M4	7 e 8	Triagem de tratamentos que exigem AIPD	2 h	3 h	5 h
M5	9 e 10	Descrição do tratamento e proporcionalidade	2 h	3 h	5 h
M6	11 e 12	Avaliação de risco na AIPD e medidas	2 h	3 h	5 h
M7	13 e 14	Relatório de AIPD e consulta prévia	2 h	3 h	5 h
M8	15 e 16	Oficina de violação de dados pessoais	2 h	3 h	5 h
M9	17 e 18	Oficina de AIPD com base no RAT	2 h	3 h	5 h
M10	19 e 20	Projeto final: avaliação integrada do percurso	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 — Detecção e caracterização de violações de dados (5 horas)

- Violação de dados pessoais na aceção do RGPD e distinção de incidente de segurança genérico.
- Confidencialidade, integridade e disponibilidade aplicadas aos dados pessoais.
- Canais de detecção, triagem, contenção e responsabilidades iniciais.
- Factos confirmados versus pressupostos e necessidade de registo cronológico.

Atividade prática: Classificar cinco ocorrências fictícias e estabelecer a cronologia de uma violação.

Evidência de aprendizagem: Ficha de triagem e registo cronológico de ocorrência.

M2 — Risco para os titulares e decisão de notificação (5 horas)

- Consequências materiais e imateriais para direitos e liberdades.
- Critério de risco para notificação à autoridade de controlo.
- Artigo 33.º: conteúdo e prazo de 72 horas, quando aplicável, a contar do conhecimento.
- Notificação faseada quando não é possível dispor de todos os elementos de imediato.

Atividade prática: Aplicar critérios a três incidentes simulados e redigir decisão fundamentada.

Evidência de aprendizagem: Fichas de decisão e minuta de notificação à CNPD.

M3 — Comunicação a titulares e documentação (5 horas)

- Critério de risco elevado para comunicação aos titulares (artigo 34.º).
- Conteúdo de comunicação clara e útil para os afectados.
- Documentação interna de todas as violações, notificadas ou não.
- Medidas correctivas, responsáveis e preservação de evidências.

Atividade prática: Preparar comunicação a titulares e completar registo de violação simulada.

Evidência de aprendizagem: Comunicação, registo interno e plano de medidas correctivas.

M4 — Triagem de tratamentos que exigem AIPD (5 horas)

- AIPD no artigo 35.º; finalidade preventiva e momento adequado.
- Critérios de susceptibilidade de elevado risco e orientações aplicáveis.
- Análise dos tratamentos já documentados no RAT da ação 5.
- Registo de fundamentação para realizar ou dispensar AIPD.

Atividade prática: Triar as actividades já incluídas no RAT, sem efectuar novo mapeamento integral.

Evidência de aprendizagem: Grelha de selecção de tratamentos para AIPD.

M5 — Descrição do tratamento e proporcionalidade (5 horas)

- Componentes de uma AIPD: descrição sistemática e finalidades.
- Necessidade, adequação e proporcionalidade das operações previstas.
- Categorias de dados, destinatários, tecnologias e intervenientes.
- Consulta interna e contributos de responsáveis e EPD quando aplicável.

Atividade prática: Descrever um tratamento do RAT e justificar a sua necessidade e proporcionalidade.

Evidência de aprendizagem: Secções iniciais da AIPD com fluxos e fundamentos documentados.

M6 — Avaliação de risco na AIPD e medidas (5 horas)

- Riscos próprios dos titulares: discriminação, perda de controlo e exposição indevida.
- Probabilidade e gravidade avaliadas com critérios apropriados ao tratamento.
- Medidas técnicas e organizativas que protegem as pessoas; riscos remanescentes.
- Distinção de uma AIPD da avaliação de segurança dos ativos da ação 1.

Atividade prática: Construir avaliação para um tratamento de risco elevado e propor medidas.

Evidência de aprendizagem: Grelha específica de riscos da AIPD e plano de mitigação.

M7 — Relatório de AIPD e consulta prévia (5 horas)

- Estrutura do relatório: tratamento, proporcionalidade, riscos e salvaguardas.

- Responsáveis pelas decisões, aprovação e revisão antes de alterações relevantes.
- Artigo 36.º: enquadramento da consulta prévia nos casos aplicáveis.
- Limitações da análise e encaminhamento de dúvidas para os responsáveis competentes.

Atividade prática: Redigir relatório preliminar e assinalar decisões pendentes.

Evidência de aprendizagem: Minuta de AIPD com conclusões e justificações.

M8 — Oficina de violação de dados pessoais (5 horas)

- Simulação de incidente que afecta serviço externo e dados de clientes.
- Linha temporal, informação disponível e decisão sobre notificação.
- Coordenação entre equipas técnicas, EPD e responsáveis pelo tratamento.
- Registo de comunicação, medidas imediatas e lições aprendidas.

Atividade prática: Realizar simulação de uma violação ligada a fornecedor do caso transversal.

Evidência de aprendizagem: Dossier de ocorrência com decisões e documentação de suporte.

M9 — Oficina de AIPD com base no RAT (5 horas)

- Selecção justificada de operação sujeita a AIPD.
- Consolidação da descrição e análise de proporcionalidade.
- Revisão entre pares dos riscos para os titulares e das medidas propostas.
- Verificação de consistência com o RAT, os avisos e os controlos existentes.

Atividade prática: Rever e completar AIPD de tratamento já mapeado na ação 5.

Evidência de aprendizagem: AIPD revista e grelha de controlo cruzado.

M10 — Projeto final: avaliação integrada do percurso (5 horas)

- Conclusão do dossier de notificação, comunicação e AIPD.
- Articulação com inventário, acessos, fornecedores e planos de continuidade.
- Discussão da diferença entre falha técnica, risco organizacional e risco para titulares.
- Apresentação individual, identificação de lacunas e prioridades de melhoria.

Atividade prática: Defender perante o formador uma decisão de notificação e uma AIPD documentada.

Evidência de aprendizagem: Dossier final: registo de violação, decisões, minutas, AIPD e síntese integrada.

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: Registo completo de violação, fichas de decisão, minuta de notificação, comunicação aos titulares, triagem de RAT e AIPD final.

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%

Crítérios de classificação do projeto

Crítério	Peso no projeto (%)
Triagem e documentação da violação	20%
Fundamentação de notificação e comunicação	20%
Triagem e proporcionalidade da AIPD	20%
Riscos para os titulares e medidas propostas	30%
Integração documental e defesa	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

Encerra o percurso e utiliza elementos das ações 1 a 5. O projecto final demonstra articulação de conhecimentos, sem introduzir matéria nova nem exigir competência jurídica ou técnica avançada.

Recursos e materiais

- Cenários de violação fictícios, modelos de comunicação e minuta de notificação.
- RAT e avisos produzidos na ação 5, diagramas e relatórios das ações anteriores.
- Texto do RGPD, orientações do EDPB e CNPD, editor de texto e folhas de cálculo.

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

- Registo da violação: ocorrência, conhecimento, dados, titulares, consequências, decisão, acções e evidências.
- Ficha de triagem: operação do RAT, critério de risco elevado, decisão e fundamentação.
- AIPD: descrição, necessidade, proporcionalidade, riscos para titulares, medidas, risco remanescente e validação.

Referências técnicas e normativas

Parlamento Europeu & Conselho da União Europeia. (2016). Regulamento (UE) 2016/679, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, L 119, 1–88. <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>

Comité Europeu para a Proteção de Dados. (2023). Orientações 9/2022 sobre a notificação da violação de dados pessoais ao abrigo do RGPD (versão 2.0). https://www.edpb.europa.eu/documents/guideline/guidelines-92022-on-personal-data-breach-notification-under-gdpr_pt

Comissão Nacional de Proteção de Dados. (s.d.). Orientações e recursos institucionais sobre proteção de dados pessoais. <https://www.cnpd.pt/>

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.