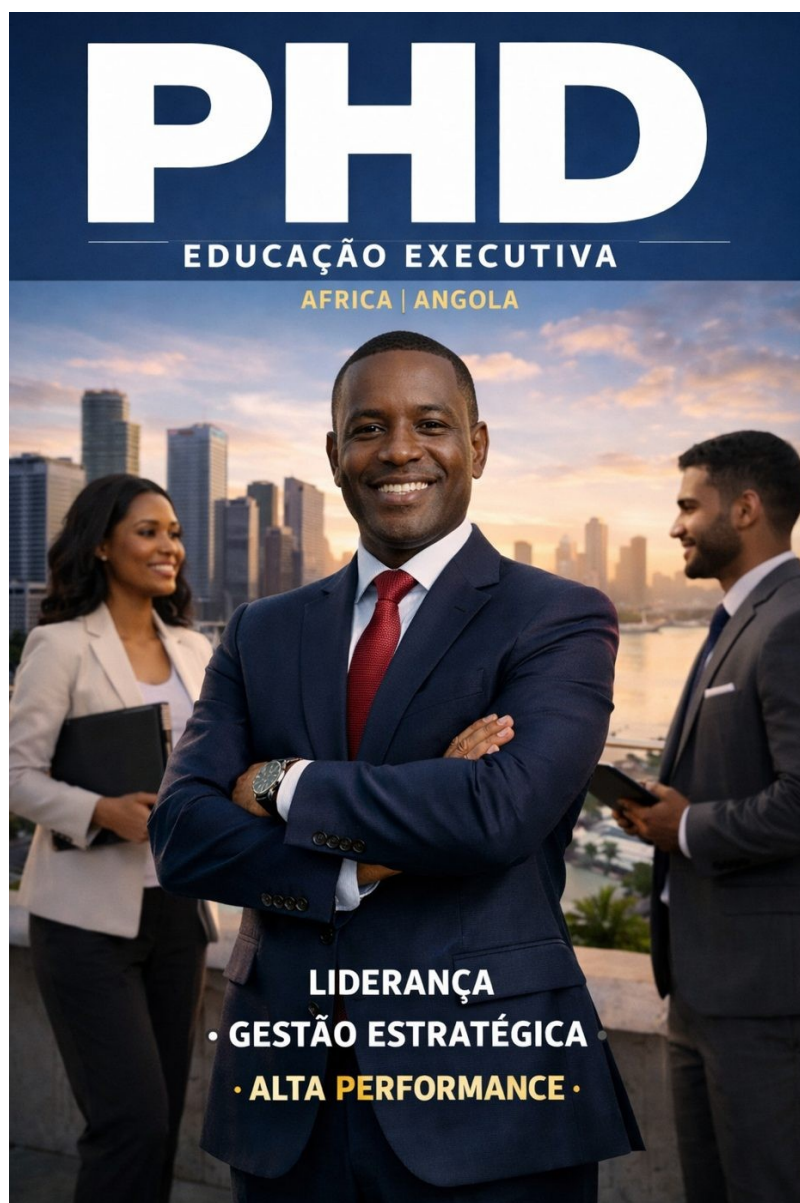




PHD EDUCAÇÃO EXECUTIVA

Portefólio de Formações Avançadas

Tecnologia, Cibersegurança, Inteligência Artificial e Governação Pública



Caderno de Programas • Luanda • Setembro de 2026

Índice

Apresentação do Portefólio

A PHD Educação Executiva, instituição de formação executiva da PHD Angola Consulting, apresenta um portefólio de oito formações avançadas nas áreas de auditoria, risco, cibersegurança, infra-estruturas de data center, inteligência artificial e governação pública.

Os programas respondem a uma necessidade concreta do mercado angolano: a digitalização acelerada da economia e do Estado aumentou a dependência de sistemas de informação, a exposição a ameaças cibernéticas e a exigência regulamentar, sem que a oferta de quadros especializados acompanhasse esse ritmo. A aprovação, em Dezembro de 2025, da Estratégia Nacional de Cibersegurança e do Conselho Nacional de Cibersegurança reforça a urgência de formar competências nacionais.

Princípios comuns a todos os programas

- Contextualização angolana: casos, quadro normativo e desafios sectoriais nacionais.
- Alinhamento com referenciais internacionais (ISO, NIST, COBIT, ITIL, IIA) nas versões em vigor.
- Forte componente prática: laboratórios, simulações, Cyber Range e projecto final integrador.
- Estrutura modular e escalável: níveis de 40 a 120 horas, em regime presencial, online ou híbrido.
- Preparação para certificações internacionais reconhecidas pelo mercado.
- Disponibilidade em formato aberto ou in-company, adaptado às necessidades de cada organização.

Estrutura de cada ficha de programa

Cada programa é apresentado segundo a mesma estrutura: 1. Justificação · 2. Enquadramento · 3. Objectivos · 4. Público-alvo · 5. Oferta Formativa (módulos, componente prática, projecto final, competências, duração, metodologia, certificações e resultado esperado).

Quadro-síntese

Código	Programa	Público principal	Duração
FA-01	Formação Avançada em Auditoria, Risco e Cibersegurança	Auditores internos e externos; Gestores de risco; Responsáveis de compliance e controlo interno	40 h · 60 h · 80 h
FA-02	Formação Avançada em Cibersegurança e Segurança da Informação	Responsáveis de Segurança da Informação (CISO/RSI); Administradores de sistemas e redes; Profissionais de TI	60 h · 80 h
FA-03	Formação Avançada em Resposta e Análise Forense de Incidentes de Cibersegurança	Analistas SOC (N1-N3) e threat hunters; Membros de equipas CSIRT/CERT; Administradores de sistemas e redes	40 h · 60 h · 80 h · 100 h
FA-04	Formação Avançada em Gestão de Infra-estruturas de Data Center	Engenheiros de infra-estruturas e facilities; Administradores de sistemas, redes e storage; Gestores e directores de TI	40 h · 60 h · 80 h · 100 h
FA-05	Formação Avançada em Cibersegurança Aplicada à Segurança Pública	Oficiais e quadros das forças de segurança e ordem pública; Órgãos de polícia criminal e investigação; Protecção civil e serviços de emergência	40 h · 60 h · 80 h · 120 h

Código	Programa	Público principal	Duração
FA-06	Formação Avançada em Inteligência Artificial e Engenharia de Prompts	Gestores e quadros técnicos; Profissionais de TI, dados e inovação; Consultores e analistas de negócio	40 h · 60 h · 80 h · 120 h
FA-07	Formação Executiva Avançada em Gestão Empresarial e Inteligência Artificial	Administradores e directores-gerais; Gestores executivos e empresários; Directores de tecnologia (CIO/CTO)	40 h · 60 h · 80 h · 120 h
FA-08	Formação Avançada em Inteligência Aplicada à Administração Pública e Local: Políticas Públicas, Governação e Transformação Digital	Dirigentes da Administração Pública; Administradores municipais e quadros da administração local; Técnicos superiores do Estado	40 h · 60 h · 80 h · 120 h

FA-01 · Auditoria, Risco e Cibersegurança

FORMAÇÃO AVANÇADA EM AUDITORIA, RISCO E CIBERSEGURANÇA

Da gestão do risco empresarial à auditoria de sistemas de informação: uma visão integrada de governação, controlo e segurança.

1. Justificação

O risco tecnológico passou a ser risco de negócio. A digitalização dos serviços financeiros, das telecomunicações e da Administração Pública aumentou a exposição das organizações angolanas a fraude, falhas operacionais e ataques cibernéticos, com impacto directo na continuidade, na reputação e na conformidade regulamentar.

As funções de auditoria interna, gestão de risco e compliance necessitam de quadros capazes de avaliar controlos tecnológicos com o mesmo rigor com que avaliam controlos financeiros — competência ainda escassa no mercado nacional.

2. Enquadramento

O programa articula as três linhas de defesa e alinha-se com os referenciais internacionais de auditoria, risco e segurança, contextualizados no quadro normativo angolano aplicável aos sectores regulados.

Referenciais normativos e de boas práticas

- IIA — Global Internal Audit Standards (2024)
- COSO Controlo Interno e COSO ERM
- ISO 31000 · ISO/IEC 27001:2022 · ISO/IEC 27005
- NIST Cybersecurity Framework 2.0 · COBIT 2019
- Lei n.º 22/11 (Protecção de Dados Pessoais) · Lei n.º 7/17 (Protecção das Redes e Sistemas Informáticos)
- BNA — Aviso n.º 08/2020 (Segurança Cibernética e Computação em Nuvem)

3. Objectivos

Objectivo geral

Capacitar profissionais para identificar, avaliar e mitigar riscos organizacionais, executar auditorias baseadas no risco e verificar a eficácia dos controlos de cibersegurança.

Objectivos específicos

No final da formação, os participantes serão capazes de:

- ✓ Aplicar princípios de governação corporativa e o modelo das três linhas.
- ✓ Estruturar processos de Enterprise Risk Management (ERM).
- ✓ Planear e executar auditorias baseadas no risco.
- ✓ Avaliar controlos de segurança e de sistemas de informação.
- ✓ Apoiar a conformidade regulamentar e a prevenção da fraude.
- ✓ Produzir relatórios executivos com recomendações accionáveis.

4. Público-alvo

- Auditores internos e externos
- Gestores de risco
- Responsáveis de compliance e controlo interno
- Profissionais de TI e segurança da informação
- Gestores e executivos envolvidos em governação corporativa

5. Oferta Formativa

5.1 Estrutura modular

Módulo	Conteúdos	Componente prática
M1 Fundamentos de Auditoria e Governação	• Conceitos e princípios de auditoria • Modelos de governação corporativa • Modelo das três linhas • Ética e independência do auditor • Normas internacionais de auditoria	<i>Integrada nos casos e exercícios do módulo</i>
M2 Gestão de Riscos Empresariais	• Enterprise Risk Management (ERM) • Identificação e classificação de riscos • Análise qualitativa e quantitativa • Apetite e tolerância ao risco • Matriz de riscos e controlos	<i>Integrada nos casos e exercícios do módulo</i>
M3 Auditoria Baseada no Risco	• Planeamento da auditoria • Avaliação do controlo interno • Testes de conformidade e substantivos • Evidências de auditoria • Relatórios e recomendações	<i>Integrada nos casos e exercícios do módulo</i>
M4 Fundamentos de Cibersegurança	• Tríade CIA: confidencialidade, integridade e disponibilidade • Ameaças e vulnerabilidades • Malware, ransomware e phishing • Segurança de redes • Segurança em cloud	<i>Integrada nos casos e exercícios do módulo</i>
M5 Gestão de Riscos de Cibersegurança	• NIST Cybersecurity Framework 2.0 • ISO/IEC 27001 e ISO/IEC 27005 • Avaliação da maturidade de segurança • Gestão de terceiros e fornecedores • Continuidade de negócio e recuperação de desastres	<i>Integrada nos casos e exercícios do módulo</i>
M6 Auditoria de Sistemas de Informação	• Auditoria de infra-estruturas de TI • Gestão de identidades e acessos • Auditoria de bases de dados • Auditoria de aplicações • Recolha e análise de evidências digitais	<i>Integrada nos casos e exercícios do módulo</i>
M7 Compliance e Regulamentação	• Protecção de dados e privacidade • Requisitos regulamentares sectoriais • Gestão da conformidade • Controlo interno e prevenção da fraude	<i>Integrada nos casos e exercícios do módulo</i>
M8 Resposta a Incidentes e Investigação	• Gestão de incidentes de segurança • Forense digital • Análise de logs • Comunicação de crise • Lições aprendidas e melhoria contínua	<i>Integrada nos casos e exercícios do módulo</i>

5.2 Caso Prático Final

Cada participante ou grupo deverá:

1. Identificar os riscos de uma organização.
2. Elaborar a matriz de riscos.
3. Avaliar os controlos existentes.
4. Realizar uma auditoria de cibersegurança.
5. Produzir um relatório executivo com recomendações.

5.3 Competências desenvolvidas

- Avaliação de riscos empresariais e tecnológicos
- Condução de auditorias internas
- Verificação de controlos de segurança
- Gestão da conformidade e governação
- Resposta a incidentes cibernéticos
- Elaboração de relatórios executivos

5.4 Duração e metodologia

Nível	Carga horária	Componente metodológica	Peso
Intensivo	40 h	Teoria	35%
Profissional	60 h	Laboratórios e casos	45%
Avançado c/ laboratórios	80 h	Caso prático final	20%

Modalidade: presencial, online ou híbrida.

5.5 Certificações complementares recomendadas

- ISO/IEC 27001 Lead Auditor
- ISO/IEC 27001 Lead Implementer
- CISA
- CRISC
- CISSP
- COBIT 2019 Foundation
- CIA — Certified Internal Auditor

RESULTADO ESPERADO

Profissionais capazes de integrar funções de auditoria interna, gestão de risco e compliance com domínio técnico dos riscos tecnológicos e de cibersegurança.

FA-02 · Cibersegurança e Segurança da Informação

FORMAÇÃO AVANÇADA EM CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO

Competências avançadas para proteger sistemas, redes, dados e infra-estruturas críticas segundo as melhores práticas internacionais.

1. Justificação

A frequência e a sofisticação dos ataques — ransomware, fraude digital, comprometimento de contas e exfiltração de dados — crescem mais depressa do que a capacidade das organizações para formar e reter especialistas.

Em Angola, a aprovação da Estratégia Nacional de Cibersegurança (2025) e as exigências do regulador financeiro tornam a segurança da informação uma obrigação de gestão, e não apenas uma função técnica.

2. Enquadramento

Programa técnico-estratégico estruturado em torno de um Sistema de Gestão de Segurança da Informação (SGSI), cobrindo o ciclo completo: governação, risco, protecção, detecção, resposta e auditoria.

Referenciais normativos e de boas práticas

- ISO/IEC 27001:2022 e ISO/IEC 27002:2022
- ISO/IEC 27005 (gestão do risco)
- NIST Cybersecurity Framework 2.0
- CIS Critical Security Controls v8
- Decreto Presidencial n.º 256/25 (Estratégia Nacional de Cibersegurança)
- Lei n.º 7/17 · Lei n.º 22/11 · BNA Aviso n.º 08/2020

3. Objectivos

Objectivo geral

Formar especialistas capazes de conceber, implementar e gerir programas de segurança da informação alinhados com normas internacionais e com o contexto regulamentar angolano.

Objectivos específicos

No final da formação, os participantes serão capazes de:

- ✓ Compreender o panorama actual das ciberameaças.
- ✓ Implementar e manter um SGSI.
- ✓ Gerir riscos de cibersegurança.
- ✓ Aplicar normas e frameworks internacionais.
- ✓ Realizar avaliações de vulnerabilidades.
- ✓ Gerir incidentes de segurança.
- ✓ Desenvolver políticas e controlos de segurança.
- ✓ Apoiar processos de conformidade e auditoria.

4. Público-alvo

- Responsáveis de Segurança da Informação (CISO/RSI)
- Administradores de sistemas e redes
- Profissionais de TI
- Gestores de risco

- Auditores de sistemas de informação
- Consultores de segurança
- Técnicos de infra-estruturas tecnológicas

5. Oferta Formativa

5.1 Estrutura modular

Módulo	Conteúdos	Componente prática
M1 Fundamentos de Cibersegurança	• Tríade CIA • Activos de informação • Vectores de ataque • Panorama global das ciberameaças • Tendências tecnológicas	Exercícios <i>Identificação de activos críticos</i> <i>Classificação da informação</i>
M2 Gestão de Segurança da Informação	• SGSI — ISO/IEC 27001 e 27002 • Estrutura de políticas • Gestão documental • Cultura de segurança	Laboratório <i>Política de Segurança da Informação</i>
M3 Gestão de Riscos em Cibersegurança	• ISO/IEC 27005 • Metodologias de avaliação • Ameaças e vulnerabilidades • Avaliação de impacto • Tratamento do risco	Laboratório <i>Matriz de riscos</i> <i>Plano de tratamento de riscos</i>
M4 Segurança de Redes e Infra-estruturas	• Arquitecturas seguras • Firewalls e IDS/IPS • VPN e segmentação • Ambientes híbridos	Prática <i>Políticas de segurança de rede</i> <i>Análise de tráfego suspeito</i>
M5 Gestão de Identidades e Acessos (IAM)	• Controlo de acessos • Autenticação multifactor (MFA) • Gestão de acessos privilegiados (PAM) • Single Sign-On (SSO) • Zero Trust	Laboratório <i>Implementação de MFA</i> <i>Análise de privilégios críticos</i>
M6 Segurança em Cloud Computing	• Modelos SaaS, PaaS e IaaS • Responsabilidade partilhada • Segurança em Azure, AWS e Google Cloud • Protecção de dados em cloud	Laboratório <i>Configuração segura de serviços cloud</i>
M7 Ethical Hacking e Gestão de Vulnerabilidades	• Ciclo do ethical hacking • Reconhecimento e scanning • Exploração controlada • Gestão de vulnerabilidades • Hardening de sistemas	Laboratório <i>Análise de vulnerabilidades</i> <i>Relatório técnico</i>
M8 Resposta a Incidentes e Forense Digital	• Ciclo de gestão de incidentes • Detecção e análise • Contenção, erradicação e recuperação • Preservação de evidências digitais	Laboratório <i>Simulação de ransomware</i> <i>Plano de resposta a incidentes</i>

Módulo	Conteúdos	Componente prática
M9 Segurança de Dados e Privacidade	• Classificação de dados • Protecção de dados pessoais • Criptografia e gestão de chaves • Data Loss Prevention (DLP)	Exercícios <i>Mecanismos de protecção de dados</i>
M10 Compliance e Auditoria de Segurança	• Auditoria de segurança da informação • Avaliação de conformidade • NIST CSF 2.0 e COBIT 2019 • Gestão de evidências • Indicadores de conformidade	Laboratório <i>Planeamento e execução de auditoria</i>

5.2 Projecto Final Integrador

Cada participante ou grupo deverá:

1. Identificar os activos críticos de uma organização.
2. Realizar a avaliação de riscos.
3. Definir e implementar controlos de segurança.
4. Elaborar políticas de segurança.
5. Desenvolver um plano de resposta a incidentes.
6. Produzir um relatório executivo com recomendações.

5.3 Competências desenvolvidas

- Gestão e governação da segurança da informação
- Análise e tratamento de riscos
- Protecção de infra-estruturas tecnológicas
- Implementação de controlos de segurança
- Gestão de incidentes cibernéticos
- Auditoria de sistemas de informação
- Conformidade com normas internacionais
- Protecção de dados e privacidade

5.4 Duração e metodologia

Nível	Carga horária	Componente metodológica	Peso
Profissional	60 h	Teoria	35%
Avançado	80 h	Laboratórios práticos	45%
		Projecto integrador	20%

Modalidade: presencial, online ou híbrida.

5.5 Certificações complementares recomendadas

- ISO/IEC 27001 Lead Implementer
- ISO/IEC 27001 Lead Auditor
- CompTIA Security+
- CompTIA CySA+
- CEH — Certified Ethical Hacker
- CISSP
- CISM
- CRISC

- CISA
- Microsoft Cybersecurity Architect Expert (SC-100)

RESULTADO ESPERADO

Especialistas de nível intermédio e avançado para bancos, seguradoras, operadores de telecomunicações, organismos públicos, academias e centros de formação.

FA-03 · Resposta e Análise Forense de Incidentes de Cibersegurança

FORMAÇÃO AVANÇADA EM RESPOSTA E ANÁLISE FORENSE DE INCIDENTES DE CIBERSEGURANÇA

Detectar, conter, investigar e documentar incidentes com rigor técnico e valor probatório.

1. Justificação

Quando um incidente ocorre, o tempo de detecção e a qualidade da resposta determinam a dimensão do prejuízo. A maioria das organizações não dispõe de equipas preparadas para preservar evidências, reconstruir o ataque e sustentar decisões técnicas, regulamentares e judiciais.

A criação do Conselho Nacional de Cibersegurança e o reforço das capacidades nacionais de resposta (CSIRT/CERT) exigem profissionais com formação especializada em incident handling e forense digital.

2. Enquadramento

Formação altamente prática, assente em laboratórios e num Cyber Range, que segue o ciclo de resposta a incidentes e as boas práticas de cadeia de custódia aplicáveis à prova digital.

Referenciais normativos e de boas práticas

- NIST SP 800-61 Rev. 3 (2025) — perfil CSF 2.0
- ISO/IEC 27035 (gestão de incidentes)
- ISO/IEC 27037 (recolha e preservação de prova digital)
- SANS PICERL · MITRE ATT&CK
- Código Penal angolano (Lei n.º 38/20) — criminalidade informática
- Decreto Presidencial n.º 258/25 (Conselho Nacional de Cibersegurança)

3. Objectivos

Objectivo geral

Desenvolver competências especializadas na detecção, resposta, investigação e análise forense de incidentes, minimizando impactos, preservando evidências e apoiando a recuperação e a conformidade.

Objectivos específicos

No final da formação, os participantes serão capazes de:

- ✓ Identificar e analisar incidentes de cibersegurança.
- ✓ Aplicar metodologias de resposta a incidentes.
- ✓ Preservar e recolher evidências digitais.
- ✓ Realizar análises forenses em sistemas, memória e redes.
- ✓ Investigar actividades maliciosas e comprometimentos.
- ✓ Elaborar relatórios técnicos e periciais.
- ✓ Apoiar a recuperação e a melhoria contínua.

4. Público-alvo

- Analistas SOC (N1–N3) e threat hunters
- Membros de equipas CSIRT/CERT
- Administradores de sistemas e redes
- Investigadores de cibercrime e peritos digitais

- Auditores de SI e responsáveis de segurança
- Quadros de órgãos de polícia criminal e de regulação

5. Oferta Formativa

5.1 Estrutura modular

Módulo	Conteúdos	Componente prática
M1 Fundamentos de Resposta a Incidentes	• Conceito e tipologia de incidentes • Ciclo de vida dos incidentes • Estrutura de uma equipa CSIRT/CERT • NIST SP 800-61 · ISO/IEC 27035 · SANS	Exercício <i>Classificação e categorização de incidentes</i>
M2 Gestão e Coordenação de Incidentes	• Preparação e planos de resposta • Gestão de crises cibernéticas • Escalonamento • Comunicação interna e externa • Gestão de stakeholders	Laboratório <i>Plano de Resposta a Incidentes (PRI)</i>
M3 Deteção e Análise Inicial	• Indicadores de compromisso (IoC) e de ataque (IoA) • Monitorização, SIEM e SOC • Correlação de eventos • Threat intelligence • Ferramentas: Microsoft Sentinel, Splunk, Elastic, Wazuh	Laboratório <i>Investigação de alertas de segurança</i>
M4 Preservação e Cadeia de Custódia	• Enquadramento legal da prova digital • Cadeia de custódia • Integridade da evidência — hashing • Procedimentos de recolha	Laboratório <i>Recolha e preservação de evidências</i>
M5 Forense em Sistemas Operativos	• Windows: registo, event logs, Prefetch, ficheiros LNK, timeline • Linux: logs, processos, histórico de comandos, persistência • Ferramentas: FTK Imager, Autopsy, Velociraptor, KAPE	Laboratório <i>Investigação de sistema comprometido</i>
M6 Forense de Memória	• Aquisição de memória RAM • Processos maliciosos e rootkits • Malware residente em memória • Credenciais em memória • Ferramentas: Volatility 3, MemProcFS	Laboratório <i>Extracção e análise de artefactos</i>
M7 Forense de Redes	• Captura e análise de tráfego • Reconstrução de sessões • Deteção de exfiltração • Análise de protocolos • Ferramentas: Wireshark, tcpdump, Zeek, NetworkMiner	Laboratório <i>Investigação de tráfego suspeito</i>

Módulo	Conteúdos	Componente prática
M8 Análise de Malware	- Tipos e comportamento de malware - Engenharia reversa básica - Indicadores de infecção - Sandboxing: ANY.RUN, CAPE, PEStudio, VirusTotal	Laboratório <i>Análise comportamental de malware</i>
M9 Investigação de Ataques Avançados	- Ransomware e Business Email Compromise - Ameaças persistentes avançadas (APT) - Movimento lateral e persistência - Exfiltração de dados	Exercício <i>Investigação completa de ataque ransomware</i>
M10 Forense em Cloud e Ambientes Híbridos	- Microsoft 365 e Azure - Investigação em AWS - Logs de cloud - Auditoria em ambientes híbridos	Laboratório <i>Incidente em ambiente cloud</i>
M11 Relatórios Forenses e Peritagem Digital	- Estrutura do relatório forense - Comunicação executiva - Apresentação de evidências - Conclusões técnicas e recomendações	Exercício <i>Relatório pericial completo</i>

5.2 Simulações operacionais (Cyber Range)

Os participantes enfrentarão cenários realistas envolvendo:

- Ataques de ransomware
- Phishing e comprometimento de contas
- Ameaça interna (insider threat)
- Exfiltração de dados
- Comprometimento de servidores
- Ataques a infra-estruturas críticas

5.3 Projecto Final

Cada participante ou grupo deverá:

1. Receber um cenário de incidente.
2. Recolher evidências digitais.
3. Realizar a análise forense.
4. Identificar o vector de ataque.
5. Determinar o impacto.
6. Elaborar o relatório técnico.
7. Apresentar recomendações de mitigação.

5.4 Competências desenvolvidas

- Incident handling
- Forense digital, de memória e de redes
- Análise de malware
- Threat hunting e threat intelligence
- Gestão de crises cibernéticas
- Investigação de ransomware
- Preservação de evidências digitais
- Elaboração de relatórios periciais

5.5 Duração e metodologia

Nível	Carga horária	Componente metodológica	Peso
Intensivo	40 h	Teoria	25%
Profissional	60 h	Laboratórios forenses	50%
Especialista	80 h	Cyber Range e projecto	25%
Executivo + laboratórios avançados	100 h		

Modalidade: presencial, online ou híbrida.

5.6 Certificações complementares recomendadas

- GIAC GCIH — Certified Incident Handler
- GIAC GCFA — Certified Forensic Analyst
- GIAC GNFA — Network Forensic Analyst
- GIAC GCFE — Certified Forensic Examiner
- EC-Council CHFI
- CompTIA CySA+
- CISSP
- Microsoft Cybersecurity Architect Expert (SC-100)

RESULTADO ESPERADO

Especialistas preparados para integrar SOC, CSIRT/CERT, unidades de investigação digital e equipas de resposta a incidentes em organizações públicas e privadas.

FA-04 · Gestão de Infra-estruturas de Data Center

FORMAÇÃO AVANÇADA EM GESTÃO DE INFRA-ESTRUTURAS DE DATA CENTER

Conceber, operar e otimizar centros de dados de missão crítica com elevada disponibilidade e eficiência.

1. Justificação

A soberania digital, a digitalização do Estado e a expansão dos serviços financeiros móveis dependem de centros de dados fiáveis, seguros e energeticamente eficientes. Angola dispõe hoje de data centers certificados e de conectividade internacional por cabos submarinos, mas a oferta de quadros especializados em operação de infra-estruturas críticas não acompanha o investimento.

Falhas de energia, climatização ou capacidade traduzem-se em indisponibilidade de serviços essenciais — um risco que exige gestão profissional e certificada.

2. Enquadramento

Programa que cobre o ciclo de vida do data center — concepção, construção, operação, continuidade e governação — integrando as dimensões física, lógica e de gestão de serviços.

Referenciais normativos e de boas práticas

- ANSI/TIA-942 · Uptime Institute Tier Standards
- EN 50600 · ISO/IEC 22237
- ISO/IEC 30134 (KPI de eficiência — PUE)
- ISO 22301 (continuidade de negócio)
- ITIL 4 · COBIT 2019
- Estratégia Nacional de Cibersegurança (DP n.º 256/25)

3. Objectivos

Objectivo geral

Formar gestores e especialistas capazes de administrar infra-estruturas de data center de missão crítica, garantindo disponibilidade, segurança e eficiência operacional.

Objectivos específicos

No final da formação, os participantes serão capazes de:

- ✓ Projectar e gerir infra-estruturas de data center.
- ✓ Garantir alta disponibilidade e continuidade dos serviços.
- ✓ Implementar boas práticas de operação e manutenção.
- ✓ Gerir energia, climatização e capacidade.
- ✓ Monitorizar e optimizar o desempenho dos recursos.
- ✓ Aplicar normas internacionais de data center.
- ✓ Implementar estratégias de recuperação de desastres.

4. Público-alvo

- Engenheiros de infra-estruturas e facilities
- Administradores de sistemas, redes e storage
- Gestores e directores de TI
- Técnicos de operação de NOC e data center

- Engenheiros electrotécnicos e de climatização
- Gestores de continuidade de negócio

5. Oferta Formativa

5.1 Estrutura modular

Módulo	Conteúdos	Componente prática
M1 Fundamentos de Data Center	• Evolução e tipologias: enterprise, colocation, hyperscale, edge • Componentes críticos • Requisitos de disponibilidade • Capacidade e escalabilidade • TIA-942 · Uptime Tier · EN 50600 · ISO/IEC 22237	Exercício <i>Avaliação da maturidade de um data center</i>
M2 Arquitetura Física	• Layout e design físico • Sala de equipamentos • Racks e bastidores • Cablagem estruturada e gestão de cabos • Zonas de segurança	Laboratório <i>Planeamento de layout</i>
M3 Energia e Sistemas Eléctricos	• Distribuição eléctrica e redundância • UPS e geradores • PDU • Sistemas de ligação à terra • PUE e eficiência energética	Laboratório <i>Cálculo de capacidade energética</i>
M4 Climatização e Ambiente	• HVAC e sistemas de arrefecimento • Corredores quentes e frios • Free cooling • Monitorização ambiental • Gestão térmica	Laboratório <i>Análise de eficiência térmica</i>
M5 Redes para Data Centers	• Arquitecturas spine-leaf • Switching e routing • SDN • Segmentação e redundância • Balanceamento de carga	Laboratório <i>Arquitectura redundante</i>
M6 Virtualização e Computação	• Virtualização de servidores • VMware vSphere, Hyper-V e KVM • Clustering • Alta disponibilidade	Laboratório <i>Cluster virtualizado</i>
M7 Armazenamento Empresarial	• SAN, NAS e DAS • Virtualização de storage • Replicação de dados • Fibre Channel, iSCSI e NVMe	Laboratório <i>Configuração de ambiente SAN</i>
M8 Monitorização e Operação	• DCIM • Gestão de capacidade e desempenho • Gestão operacional e de incidentes • Ferramentas: Zabbix, PRTG, SolarWinds, ManageEngine	Laboratório <i>Monitorização centralizada</i>

Módulo	Conteúdos	Componente prática
M9 Segurança Física e Lógica	- Controlo de acessos, CCTV e biometria - Deteção de intrusão - Segmentação, firewalls e IDS/IPS - Gestão de acessos privilegiados	Laboratório <i>Avaliação de riscos do data center</i>
M10 Continuidade e Disaster Recovery	- BCP e DRP - RTO e RPO - Site de contingência - Estratégias de recuperação	Laboratório <i>Plano de Recuperação de Desastres</i>
M11 Cloud, Híbrido e Data Centers Modernos	- Integração cloud e on-premises - Hybrid e multi-cloud - Edge computing - Software-Defined Data Center - Azure, AWS e Google Cloud	Laboratório <i>Arquitectura híbrida</i>
M12 Governança e Gestão de Serviços	- ITIL 4 e COBIT 2019 - Gestão de mudanças - Gestão de capacidade e disponibilidade - Gestão financeira do data center	Exercício <i>Definição de KPI operacionais</i>

5.2 Projecto Final Integrador

Cada participante ou grupo deverá:

1. Projectar um data center de nível empresarial.
2. Definir a arquitectura física e lógica.
3. Dimensionar energia e climatização.
4. Desenvolver estratégias de alta disponibilidade.
5. Elaborar planos de continuidade e recuperação.
6. Apresentar o plano operacional e de segurança.

5.3 Competências desenvolvidas

- Gestão de infra-estruturas de data center
- Arquitectura de centros de dados
- Virtualização e cloud híbrida
- Gestão energética
- Climatização e eficiência operacional
- Redes de alta disponibilidade
- Armazenamento empresarial
- Continuidade de negócio e disaster recovery
- Operação de infra-estruturas críticas

5.4 Duração e metodologia

Nível	Carga horária	Componente metodológica	Peso
Intensivo	40 h	Teoria	30%
Profissional	60 h	Laboratórios práticos	50%
Avançado	80 h	Projecto integrador	20%
Especialista c/ laboratórios	100 h		

Modalidade: presencial, online ou híbrida.

5.5 Certificações complementares recomendadas

- EPI CDCP · CDCS · CDCE
- Uptime Institute ATD — Accredited Tier Designer
- VMware VCP-DCV
- Microsoft Azure Administrator Associate
- AWS Certified Solutions Architect
- ITIL 4 Foundation
- COBIT 2019 Foundation

RESULTADO ESPERADO

Gestores e especialistas capazes de administrar data centers de missão crítica e suportar a transformação digital das organizações.

FA-05 · Cibersegurança Aplicada à Segurança Pública

FORMAÇÃO AVANÇADA EM CIBERSEGURANÇA APLICADA À SEGURANÇA PÚBLICA

Proteger instituições, infra-estruturas críticas e cidadãos num espaço de segurança cada vez mais digital.

1. Justificação

As forças de segurança, a protecção civil e os serviços de emergência dependem de sistemas de comunicação, bases de dados e centros de comando cuja indisponibilidade afecta directamente a ordem pública e a vida dos cidadãos.

O cibercrime, as campanhas de desinformação e os ataques a operadores de serviços essenciais exigem capacidades próprias de prevenção, investigação e resposta nas instituições do Estado, em articulação com o novo modelo nacional de governação da cibersegurança.

2. Enquadramento

Programa orientado para o contexto institucional público e policial, que integra protecção de infra-estruturas críticas, operação de SOC, investigação digital e gestão de crises com coordenação interinstitucional.

Referenciais normativos e de boas práticas

- Decreto Presidencial n.º 256/25 — Estratégia Nacional de Cibersegurança
- Decreto Presidencial n.º 258/25 — Conselho Nacional de Cibersegurança
- Lei n.º 7/17 · Lei n.º 22/11 · Código Penal (Lei n.º 38/20)
- Convenção da União Africana (Malabo) sobre Cibersegurança
- NIST CSF 2.0 · ISO/IEC 27001 · ISO 22301
- NIST SP 800-61 Rev. 3 · ISO/IEC 27035

3. Objectivos

Objectivo geral

Capacitar profissionais do sector público e das forças de segurança para prevenir, detectar, responder e investigar incidentes cibernéticos com impacto na segurança pública e nas infra-estruturas críticas nacionais.

Objectivos específicos

No final da formação, os participantes serão capazes de:

- ✓ Compreender as ameaças que afectam organismos públicos e forças de segurança.
- ✓ Proteger infra-estruturas críticas e serviços essenciais.
- ✓ Implementar estratégias de cibersegurança institucional.
- ✓ Responder a incidentes com impacto na segurança nacional.
- ✓ Realizar investigações digitais e análise forense.
- ✓ Combater o cibercrime e apoiar a investigação criminal.
- ✓ Desenvolver planos de continuidade operacional e de gestão de crises.

4. Público-alvo

- Oficiais e quadros das forças de segurança e ordem pública
- Órgãos de polícia criminal e investigação
- Protecção civil e serviços de emergência
- Entidades governamentais e reguladores

- Operadores de infra-estruturas críticas
- Responsáveis de TI e segurança no sector público

5. Oferta Formativa

5.1 Estrutura modular

Módulo	Conteúdos	Componente prática
M1 Cibersegurança para a Segurança Pública	• Panorama global das ciberameaças • Cibercrime e ciberterrorismo • Guerra cibernética • Segurança nacional e ciberespaço	Casos de estudo <i>Ataques a organismos governamentais e infra-estruturas críticas</i>
M2 Protecção de Infra-estruturas Críticas	• Energia, telecomunicações e transportes • Saúde, água e saneamento • Sistemas financeiros • NIST CSF 2.0 · ISO/IEC 27001 · ISO 22301	Exercício <i>Avaliação de riscos em infra-estruturas críticas</i>
M3 Gestão de Riscos e Resiliência Cibernética	• Ameaças e vulnerabilidades • Análise de impacto operacional • Estratégias de mitigação • Resiliência organizacional	Laboratório <i>Matriz de riscos para entidades públicas</i>
M4 Segurança de Redes Governamentais	• Arquitecturas seguras e segmentação • Firewalls, IDS/IPS e VPN • Monitorização contínua	Laboratório <i>Controlos de segurança de rede</i>
M5 Centros de Operações de Segurança (SOC)	• Estrutura e funcionamento do SOC • Detecção, correlação e gestão de alertas • Threat intelligence • Microsoft Sentinel, Splunk, Wazuh, Elastic	Laboratório <i>Análise de eventos em ambiente SOC</i>
M6 Resposta a Incidentes de Segurança	• Planeamento da resposta • Equipas CSIRT/CERT • Gestão de crises e comunicação institucional • Contenção e recuperação	Simulação <i>Ransomware numa entidade pública</i>
M7 Investigação Digital e Análise Forense	• Preservação e cadeia de custódia • Forense em computadores e dispositivos móveis • Forense de rede e cloud • Autopsy, FTK Imager, Volatility, Wireshark	Laboratório <i>Intrusão em sistema governamental</i>
M8 Combate ao Cibercrime	• Tipologias de cibercrime • Fraude electrónica e crimes financeiros digitais • Ransomware e phishing • Recolha de prova digital	Exercício <i>Cenários de investigação criminal digital</i>
M9 Protecção de Dados e Privacidade	• Dados pessoais sensíveis • Classificação da informação • Criptografia e gestão de acessos • Políticas de protecção de dados	Laboratório <i>Controlos de protecção da informação</i>

Módulo	Conteúdos	Componente prática
M10 Vigilância e Tecnologias Emergentes	- IA aplicada à segurança - Vigilância digital e redes sociais (OSINT) - IoT, drones e sistemas autónomos - Cidades inteligentes seguras - Direitos fundamentais e proporcionalidade	Caso prático <i>Riscos tecnológicos em cidades inteligentes</i>
M11 Continuidade Operacional e Gestão de Crises	- Business Continuity Management - Disaster recovery e contingência - Comunicação de crise - Coordenação interinstitucional	Exercício <i>Ciberataque a serviços públicos</i>
M12 Estratégia Nacional de Cibersegurança	- Governança da cibersegurança - Políticas públicas de segurança digital - Cooperação internacional e partilha de informação - Soberania digital	Debate <i>Desafios da cibersegurança no sector público africano</i>

5.2 Simulações operacionais (Cyber Range)

Os participantes enfrentarão cenários realistas envolvendo:

- Ataques a infra-estruturas críticas
- Comprometimento de bases de dados governamentais
- Campanhas de desinformação digital
- Ciberterrorismo
- Ransomware em serviços públicos
- Ataques a sistemas de emergência
- Comprometimento de centros de comando e controlo

5.3 Projecto Final Integrador

Cada participante ou grupo deverá:

1. Avaliar os riscos de uma entidade pública.
2. Desenvolver uma estratégia de protecção cibernética.
3. Criar planos de resposta a incidentes.
4. Realizar uma investigação digital simulada.
5. Elaborar um relatório executivo para a gestão de topo.
6. Recomendar medidas de reforço da resiliência.

5.4 Competências desenvolvidas

- Cibersegurança governamental
- Protecção de infra-estruturas críticas
- Gestão de riscos cibernéticos
- Operação de SOC
- Resposta a incidentes
- Investigação digital e forense
- Combate ao cibercrime
- Gestão de crises cibernéticas
- Segurança nacional e resiliência digital

5.5 Duração e metodologia

Nível	Carga horária	Componente metodológica	Peso
Intensivo	40 h	Teoria	35%
Profissional	60 h	Laboratórios práticos	45%
Avançado	80 h	Simulações e projecto	20%
Especialista	120 h		

Modalidade: presencial, online ou híbrida.

5.6 Certificações complementares recomendadas

- CompTIA Security+ · CySA+
- CISSP
- CEH — Certified Ethical Hacker
- GIAC GCIH
- GIAC GCFA
- Certified Cyber Crime Investigator (CCCI)
- ISO/IEC 27001 Lead Implementer
- ISO/IEC 27001 Lead Auditor

RESULTADO ESPERADO

Especialistas capazes de proteger entidades públicas, apoiar operações policiais e de investigação e reforçar a resiliência digital e a segurança pública nacional.

FA-06 · Inteligência Artificial e Engenharia de Prompts

FORMAÇÃO AVANÇADA EM INTELIGÊNCIA ARTIFICIAL E ENGENHARIA DE PROMPTS

Utilizar a IA generativa de forma produtiva, segura e responsável — do prompt ao assistente inteligente.

1. Justificação

A IA generativa tornou-se uma ferramenta de trabalho quotidiana, mas a maioria dos utilizadores explora apenas uma fracção do seu potencial e desconhece os riscos associados — fuga de informação, respostas incorrectas, enviesamento e prompt injection.

Organizações que formam as suas equipas em engenharia de prompts, automação e governação da IA obtêm ganhos de produtividade mensuráveis e reduzem a exposição a riscos legais e reputacionais.

2. Enquadramento

Programa aplicado que combina fundamentos de IA, técnicas de engenharia de prompts, desenvolvimento de assistentes (RAG e agentes) e governação, com laboratórios sobre as principais plataformas do mercado.

Referenciais normativos e de boas práticas

- ISO/IEC 42001:2023 (sistemas de gestão de IA)
- NIST AI Risk Management Framework
- OWASP Top 10 for LLM Applications
- Recomendação da UNESCO sobre a Ética da IA
- Estratégia Continental de IA da União Africana
- Lei n.º 22/11 (Protecção de Dados Pessoais)

3. Objectivos

Objectivo geral

Capacitar profissionais, gestores e decisores para a utilização estratégica da IA generativa, com domínio da engenharia de prompts, da automação inteligente e do desenvolvimento de soluções baseadas em LLM.

Objectivos específicos

No final da formação, os participantes serão capazes de:

- ✓ Compreender os fundamentos da IA moderna.
- ✓ Utilizar ferramentas de IA generativa com eficiência e segurança.
- ✓ Desenvolver prompts avançados para diferentes casos de uso.
- ✓ Automatizar tarefas e processos com IA.
- ✓ Integrar a IA nos processos organizacionais.
- ✓ Avaliar riscos, limitações e aspectos éticos.
- ✓ Conceber soluções práticas baseadas em LLM.

4. Público-alvo

- Gestores e quadros técnicos
- Profissionais de TI, dados e inovação
- Consultores e analistas de negócio
- Profissionais de RH, finanças, marketing e jurídico

- Quadros da Administração Pública
- Docentes e formadores

5. Oferta Formativa

5.1 Estrutura modular

Módulo	Conteúdos	Componente prática
M1 Fundamentos de Inteligência Artificial	• Evolução da IA • Machine learning e deep learning • Processamento de linguagem natural • Visão computacional e IA generativa • Estado actual e tendências	Exercício <i>Casos de uso de IA por sector</i>
M2 Ecosistema da IA Generativa	• LLM e modelos multimodais • Geração de texto, imagem, áudio e vídeo • Assistentes: ChatGPT, Claude, Gemini, Microsoft Copilot • IA aplicada à produtividade	Laboratório <i>Comparação prática de modelos</i>
M3 Fundamentos da Engenharia de Prompts	• Estrutura de um prompt eficaz • Contexto, objectivo, instruções e restrições • Critérios de qualidade • Zero-shot, one-shot, few-shot e role prompting	Laboratório <i>Construção e optimização de prompts</i>
M4 Engenharia de Prompts Avançada	• Raciocínio passo a passo • Prompt chaining • Self-consistency e reflexão • Meta prompting • Saídas estruturadas (JSON, tabelas)	Laboratório <i>Fluxos complexos de prompts</i>
M5 IA para Produtividade e Automação	• Automação documental e relatórios • Resumo inteligente de conteúdos • Assistentes virtuais • Aplicações em RH, finanças, saúde, educação e sector público	Laboratório <i>Assistentes de produtividade</i>
M6 IA Aplicada aos Negócios	• Transformação digital com IA • Automação de processos • Decisão inteligente • Gestão do conhecimento • Análise preditiva	Estudo de caso <i>Implementação de IA numa organização</i>
M7 Assistentes Inteligentes e Agentes	• Arquitecturas de agentes de IA • Chatbots e assistentes corporativos • Bases de conhecimento • RAG — Retrieval-Augmented Generation • Integração com ferramentas (MCP/APIs)	Laboratório <i>Assistente especializado</i>
M8 IA para Análise de Dados	• Introdução à ciência de dados • Extracção de insights • Visualização inteligente • Excel com IA, Power BI, Python, Microsoft Fabric	Laboratório <i>Dashboards com suporte de IA</i>

Módulo	Conteúdos	Componente prática
M9 IA, Segurança e Privacidade	● Prompt injection ● Fuga de dados (data leakage) ● Envenenamento de modelos ● Privacidade e segurança da informação em IA	Laboratório <i>Avaliação de riscos em aplicações de IA</i>
M10 Ética, Governança e Regulamentação	● IA responsável e transparência ● Enviesamento e discriminação ● Governança da IA — ISO/IEC 42001 ● Conformidade regulamentar ● Políticas organizacionais de IA	Exercício <i>Cenários e dilemas éticos</i>
M11 IA no Sector Público, Defesa e Segurança	● IA para serviços públicos ● IA para cibersegurança ● Análise de risco e informações ● Detecção de fraude ● Apoio à investigação digital	Caso prático <i>IA em instituições públicas</i>
M12 Projecto Final Integrador	● Identificação do problema e caso de uso ● Concepção de prompts avançados ● Assistente ou agente de IA ● Avaliação de riscos ● Apresentação de resultados	<i>Integrada nos casos e exercícios do módulo</i>

5.2 Laboratórios práticos

Os participantes trabalharão em cenários reais de:

- Criação de assistentes virtuais
- Geração automática de conteúdos
- Análise documental inteligente
- Automação de processos
- Engenharia de prompts para negócios
- IA aplicada à cibersegurança
- Bases de conhecimento inteligentes

5.3 Projecto Final Integrador

Cada participante ou grupo deverá:

1. Identificar o problema.
2. Definir o caso de uso.
3. Conceber prompts avançados.
4. Implementar um assistente ou agente de IA.
5. Avaliar os riscos.
6. Apresentar os resultados.

5.4 Competências desenvolvidas

- IA generativa
- Engenharia de prompts
- Automação inteligente
- Desenvolvimento de assistentes de IA
- Gestão do conhecimento
- Análise de dados com IA

- Transformação digital
- IA responsável e governação
- Segurança em sistemas de IA

5.5 Duração e metodologia

Nível	Carga horária	Componente metodológica	Peso
Intensivo	40 h	Fundamentos teóricos	30%
Profissional	60 h	Laboratórios práticos	50%
Avançado	80 h	Projecto aplicado	20%
Especialista	120 h		

Modalidade: presencial, online ou híbrida.

5.6 Certificações complementares recomendadas

- Microsoft Azure AI Fundamentals (AI-900)
- Microsoft Azure AI Engineer Associate (AI-102)
- Google Cloud Generative AI Leader
- AWS Certified AI Practitioner
- AWS Certified Machine Learning Engineer – Associate
- IBM AI Engineering Professional Certificate
- CertNexus Certified AI Practitioner (CAIP)

RESULTADO ESPERADO

Especialistas em IA, prompt engineers, consultores de transformação digital, analistas e arquitectos de soluções de IA, aplicando a tecnologia de forma produtiva, segura e ética.

FA-07 · Gestão Empresarial e Inteligência Artificial

FORMAÇÃO EXECUTIVA AVANÇADA EM GESTÃO EMPRESARIAL E INTELIGÊNCIA ARTIFICIAL

A IA como alavanca de estratégia, decisão, inovação e criação de valor — para quem lidera.

1. Justificação

A IA está a redefinir modelos de negócio, estruturas de custos e formas de trabalhar. A decisão de investir, onde aplicar e como governar a IA é hoje uma responsabilidade da gestão de topo, e não apenas das direcções de tecnologia.

Muitos líderes reconhecem a urgência, mas carecem de um referencial para passar da experimentação dispersa para uma estratégia com retorno mensurável, riscos controlados e equipas preparadas.

2. Enquadramento

Programa executivo, sem pré-requisitos técnicos, que integra estratégia, liderança, finanças e governação com laboratórios de aplicação directa às áreas de negócio e um projecto apresentado a um painel de administração.

Referenciais normativos e de boas práticas

- ISO/IEC 42001:2023 · NIST AI RMF
- Boas práticas de governação corporativa (OCDE)
- Business case, KPI e ROI de investimentos digitais
- Plano de Desenvolvimento Nacional 2023–2027 — transformação digital
- Lei n.º 22/11 (Protecção de Dados Pessoais)

3. Objectivos

Objectivo geral

Preparar líderes para compreender e aplicar a IA como factor estratégico de crescimento, inovação, competitividade e transformação digital das organizações.

Objectivos específicos

No final da formação, os participantes serão capazes de:

- ✓ Compreender o impacto da IA na gestão empresarial.
- ✓ Desenvolver estratégias de transformação orientadas por IA.
- ✓ Aplicar a IA à tomada de decisão executiva.
- ✓ Identificar oportunidades de automação e inovação.
- ✓ Integrar a IA nos processos de negócio.
- ✓ Gerir riscos, ética e governação da IA.
- ✓ Liderar projectos de IA com foco em resultados.

4. Público-alvo

- Administradores e directores-gerais
- Gestores executivos e empresários
- Directores de tecnologia (CIO/CTO)
- Directores financeiros e de operações
- Gestores de inovação e transformação digital
- Consultores empresariais

5. Oferta Formativa

5.1 Estrutura modular

Módulo	Conteúdos	Componente prática
M1 A Nova Era da Gestão na Economia Digital	• Evolução dos modelos de gestão • Disrupção tecnológica e competitividade • Organizações inteligentes • Liderança no contexto da IA	Caso prático <i>Empresas transformadas pela IA</i>
M2 Fundamentos de IA para Executivos	• Conceitos fundamentais de IA • Machine learning e deep learning • IA generativa e LLM • Aplicações empresariais — sem pré-requisitos técnicos	<i>Integrada nos casos e exercícios do módulo</i>
M3 Estratégia Empresarial e IA	• IA como vantagem competitiva • Estratégia digital • Planeamento baseado em dados • Roadmap de implementação	Workshop <i>Estratégia de IA para uma organização</i>
M4 Liderança na Era da IA	• Liderança digital e gestão da mudança • Novos modelos de trabalho • Cultura orientada por dados • Equipas híbridas humano-IA	Exercício <i>Maturidade digital da organização</i>
M5 Tomada de Decisão Inteligente	• Data-driven decision making • Análise preditiva • Sistemas de apoio à decisão • Microsoft Copilot, Power BI, Fabric, Azure AI	Laboratório executivo <i>Dashboards estratégicos com IA</i>
M6 IA nas Áreas de Negócio	• Marketing e vendas: personalização, comportamento do cliente • RH: recrutamento, talento, formação • Finanças: previsão, fraude, controlo orçamental • Operações: processos, logística, automação	<i>Integrada nos casos e exercícios do módulo</i>
M7 Engenharia de Prompts para Executivos	• Prompts estratégicos • Análises empresariais • Relatórios automáticos • Apoio à decisão	Laboratório <i>Prompts para estratégia, mercado, finanças, projectos e RH</i>
M8 Automação Inteligente e Produtividade	• Automação administrativa • Assistentes empresariais • Gestão documental inteligente • Automação de reuniões e conhecimento	Caso prático <i>Assistentes corporativos com IA</i>
M9 Governança, Ética e Riscos da IA	• IA responsável e ética • Enviesamento, transparência e explicabilidade • Privacidade e protecção de dados • ISO/IEC 42001 · NIST AI RMF	<i>Integrada nos casos e exercícios do módulo</i>
M10 IA para Inovação e Novos Negócios	• Novos produtos e serviços • Modelos de negócio digitais • Empreendedorismo tecnológico • Vantagem competitiva sustentável	Workshop <i>Novo modelo de negócio suportado por IA</i>

Módulo	Conteúdos	Componente prática
M11 Gestão Financeira e ROI da IA	• Avaliação de investimentos tecnológicos • Business case para IA • KPI e ROI de projectos de IA • Gestão financeira de iniciativas digitais	Laboratório <i>Business case de implementação de IA</i>
M12 Projecto Executivo Final	• Plano Estratégico de Transformação apoiado por IA • Diagnóstico, estratégia e implementação • Riscos, custos e benefícios • Apresentação à administração	<i>Integrada nos casos e exercícios do módulo</i>

5.2 Projecto Executivo Final

Cada participante ou grupo deverá:

1. Diagnóstico organizacional.
2. Identificação de oportunidades.
3. Definição da estratégia de IA.
4. Plano de implementação.
5. Avaliação de riscos.
6. Estimativa de custos e benefícios.
7. Indicadores de sucesso.
8. Apresentação à administração.

5.3 Competências desenvolvidas

- Liderança digital
- Gestão estratégica
- IA para executivos
- Transformação digital
- Engenharia de prompts
- Decisão baseada em dados
- Gestão da inovação
- Automação empresarial
- Governança da IA
- Gestão de projectos tecnológicos

5.4 Duração e metodologia

Nível	Carga horária	Componente metodológica	Peso
Executiva intensiva	40 h	Fundamentos executivos	25%
Executiva profissional	60 h	Estudos de caso	35%
Executiva avançada	80 h	Workshops práticos	25%
Programa executivo premium	120 h	Projecto estratégico	15%

Modalidade: presencial, online ou híbrida.

5.5 Certificações complementares recomendadas

- Microsoft Azure AI Fundamentals (AI-900)
- AWS Certified AI Practitioner
- Google Cloud Generative AI Leader

- PMI — Project Management Professional (PMP)
- COBIT 2019 Foundation
- ITIL 4 Foundation
- CertNexus Certified AI Practitioner (CAIP)

RESULTADO ESPERADO

Líderes preparados para conduzir a transformação digital, implementar soluções de IA, melhorar a decisão estratégica e criar modelos de negócio sustentáveis.

FA-08 · Inteligência Aplicada à Administração Pública e Local

FORMAÇÃO AVANÇADA EM INTELIGÊNCIA APLICADA À ADMINISTRAÇÃO PÚBLICA E LOCAL: POLÍTICAS PÚBLICAS, GOVERNAÇÃO E TRANSFORMAÇÃO DIGITAL

Políticas públicas baseadas em evidências, governação orientada por dados e serviços públicos digitais centrados no cidadão.

1. Justificação

A modernização do Estado, a desconcentração e a futura institucionalização das autarquias locais colocam novas exigências de planeamento, execução orçamental, prestação de contas e qualidade dos serviços prestados ao cidadão.

Dirigentes e técnicos precisam de ferramentas para formular políticas com base em evidências, monitorizar resultados e utilizar dados e IA com transparência — condição para uma Administração Pública mais eficiente e credível.

2. Enquadramento

Programa que articula inteligência estratégica, ciclo das políticas públicas, gestão por resultados e governo digital, com aplicação directa à realidade da administração central e local angolana.

Referenciais normativos e de boas práticas

- Plano de Desenvolvimento Nacional 2023–2027
- Estratégia de Longo Prazo Angola 2050
- Agenda 2063 da União Africana · ODS (Agenda 2030)
- Princípios da OCDE para a governação pública e governo digital
- Gestão por resultados e avaliação de impacto
- ISO 37001 (anti-suborno) · ISO 9001

3. Objectivos

Objectivo geral

Fortalecer as competências de dirigentes e quadros da administração central e local em inteligência estratégica, análise de políticas públicas, governação baseada em dados e transformação digital.

Objectivos específicos

No final da formação, os participantes serão capazes de:

- ✓ Conceber, implementar e avaliar políticas públicas baseadas em evidências.
- ✓ Utilizar dados, IA e análise estratégica na gestão pública.
- ✓ Melhorar o planeamento e a prestação de serviços públicos.
- ✓ Promover transparência, eficiência e inovação.
- ✓ Apoiar a governação digital e as cidades inteligentes.
- ✓ Monitorizar e avaliar o desempenho institucional.
- ✓ Aplicar boas práticas internacionais de governação.

4. Público-alvo

- Dirigentes da Administração Pública

- Administradores municipais e quadros da administração local
- Técnicos superiores do Estado
- Gestores de programas governamentais
- Deputados e assessores parlamentares
- Técnicos de planeamento e estatística
- Consultores de políticas públicas

5. Oferta Formativa

5.1 Estrutura modular

Módulo	Conteúdos	Componente prática
M1 Estado Moderno, Governação e Administração Pública	• Evolução da Administração Pública • Nova Gestão Pública • Governação colaborativa • Estado digital e modernização administrativa	Estudo de caso <i>Reformas administrativas internacionais</i>
M2 Inteligência Estratégica na Administração Pública	• Inteligência para apoio à decisão • Planeamento governamental • Análise de cenários • Gestão da informação estratégica	Laboratório <i>Cenários para decisão pública</i>
M3 Formulação e Análise de Políticas Públicas	• Ciclo das políticas públicas • Identificação de problemas e alternativas • Implementação • Avaliação de resultados e impacto	Exercício <i>Política pública sectorial</i>
M4 Gestão Baseada em Evidências e Dados	• Governo orientado por dados • Dados abertos • Business intelligence no sector público • Indicadores de desempenho • Power BI, Excel avançado, Microsoft Fabric	Laboratório <i>Dashboards para gestão pública</i>
M5 IA Aplicada ao Sector Público	• IA generativa e automação de serviços • Assistentes virtuais governamentais • Análise preditiva • Casos: educação, saúde, justiça, segurança, municípios	Laboratório <i>Soluções assistidas por IA</i>
M6 Administração Local e Governação Municipal	• Organização da administração local • Planeamento e desenvolvimento territorial • Orçamentação municipal • Participação cidadã e serviços urbanos	Exercício <i>Plano estratégico municipal</i>
M7 Cidades Inteligentes e Desenvolvimento Sustentável	• Smart cities e IoT • Mobilidade urbana inteligente • Sustentabilidade ambiental • Gestão inteligente de recursos	Projecto <i>Cidade inteligente para contexto local</i>
M8 Monitorização e Avaliação de Programas Públicos	• Indicadores e métricas • Monitorização de projectos governamentais • Avaliação de impacto • Gestão por resultados e auditoria de desempenho	Laboratório <i>Quadro de indicadores de desempenho</i>

Módulo	Conteúdos	Componente prática
M9 Transformação Digital na Administração Pública	- Governo electrónico e serviços digitais - Interoperabilidade institucional - Gestão documental electrónica e assinatura digital - Experiência do cidadão	Estudo de caso <i>Estratégias de governo digital</i>
M10 Transparência, Integridade e Boa Governação	- Ética e integridade institucional - Transparência e prestação de contas - Prevenção da corrupção - Controlo interno	Workshop <i>Plano institucional de integridade</i>
M11 Liderança e Gestão Estratégica no Sector Público	- Liderança pública e gestão da mudança - Gestão de equipas e comunicação institucional - Negociação e stakeholders - Inovação no sector público	Exercício <i>Simulação de decisão governamental</i>
M12 Projecto Final Integrador	- Diagnóstico institucional - Inteligência estratégica, ferramentas digitais e IA - Indicadores, implementação e impacto - Apresentação executiva	<i>Integrada nos casos e exercícios do módulo</i>

5.2 Projecto Final Integrador

Cada participante ou grupo deverá:

1. Diagnóstico institucional.
2. Identificação de desafios públicos.
3. Utilização de inteligência estratégica.
4. Aplicação de ferramentas digitais e IA.
5. Definição de indicadores de desempenho.
6. Plano de implementação.
7. Avaliação de impacto.
8. Apresentação executiva.

5.3 Competências desenvolvidas

- Inteligência estratégica governamental
- Formulação e avaliação de políticas públicas
- Governança e Administração Pública
- Transformação digital
- IA aplicada ao sector público
- Gestão municipal e desenvolvimento local
- Análise e visualização de dados
- Planeamento estratégico
- Gestão por resultados
- Liderança pública

5.4 Duração e metodologia

Nível	Carga horária	Componente metodológica	Peso
Executiva intensiva	40 h	Formação teórica	30%
Profissional	60 h	Estudos de caso	30%

Nível	Carga horária	Componente metodológica	Peso
Avançada	80 h	Oficinas e laboratórios	25%
Especialização superior	120 h	Projecto aplicado	15%

Modalidade: presencial, online ou híbrida.

5.5 Certificações complementares recomendadas

- Project Management Professional (PMP)
- Microsoft Power BI Data Analyst (PL-300)
- Microsoft Azure AI Fundamentals (AI-900)
- Certified Public Manager (CPM)
- COBIT 2019 Foundation
- ITIL 4 Foundation
- ISO 37001 Lead Implementer (anti-suborno)
- ISO 9001 Lead Implementer

RESULTADO ESPERADO

Quadros preparados para liderar a modernização administrativa, formular políticas baseadas em evidências e utilizar a IA para uma Administração Pública eficiente, transparente e orientada para resultados.

As Nossas Referências

Instituições públicas e privadas que confiaram na PHD Angola Consulting.

Sector Público e Regulação

 UNIDADE DE INFORMAÇÃO FINANCEIRA	 GOVERNO DE ANGOLA Ministério da Indústria e Comércio	
--	--	--

Banca e Serviços Financeiros

 BANCO SOL O banco de todos nós	 BPC O Seu Banco de Sempre	 BDA BANCO DE DESENVOLVIMENTO DE ANGOLA
 BCA Banco Comercial Angolano	 BMF BANCO BAI MICRO FINANÇAS	

Empresas e Instituições

 CLUBE DESPORTIVO 11 DE AGOSTO	 medianova	 EMPROMAD, LDA. INDÚSTRIA E COMÉRCIO GERAL
 6 PALMEIRAS COMÉRCIO E INDÚSTRIA, LDA.		

Notas e Condições

- As certificações indicadas são emitidas por entidades independentes (ISACA, ISC2, GIAC, EC-Council, CompTIA, PMI, Microsoft, AWS, Google, entre outras). Os programas preparam para os respectivos domínios de conhecimento; taxas e marcação de exames não estão incluídas, salvo acordo específico.
- As referências normativas angolanas e internacionais foram revistas em Setembro de 2026. A sua aplicação a casos concretos deve ser validada pelas áreas Jurídica e de Compliance da entidade cliente.
- Ferramentas e plataformas tecnológicas são indicativas e podem ser substituídas por equivalentes, em função do licenciamento disponível e do ambiente do cliente.
- Os conteúdos de ethical hacking, forense digital e análise de malware são leccionados em ambiente laboratorial controlado, com fins exclusivamente defensivos e sob código de conduta assinado pelos participantes.
- Carga horária, calendário e profundidade dos laboratórios são ajustáveis em formato in-company.

Contactos

E-mail: geral@phdangola.com · Telefone: +244 923 419 394 · Website: phdangola.com