bilingual edition

ptsoc {news}

Cibersegurança na Lusofonia: preparação e ameaças*

3 perguntas a António Ribeiro Head of Cybersecurity na Minsait em Portugal (Indra Group)

Mês Europeu da Cibersegurança: #THINKB4UCLICK

*Com contributos de: Angola, Brasil, Cabo Verde, Moçambique e Portugal

18

.pt

Cibersegurança na Lusofonia: preparação e ciberameaças

De acordo com o mais recente Global Cybersecurity Index divulgado pela ITU, "os ciberataques são considerados o quinto risco mais provável de causar uma crise significativa à escala global".

Sendo este um risco transversal a todos os países e regiões, poderíamos assumir que o espaço lusófono não é substancialmente diferente do resto do mundo em termos de vulnerabilidades a ciberataques e ciber-riscos em geral.

Contudo, sendo certo que não existem indicadores que sugiram existir mais ameaças na Lusofonia do que no resto do mundo, há um fator significativo em termos da vulnerabilidade destes países, o qual se prende com o grau de preparação de cada um perante este tipo de ameaças.

O mesmo relatório da ITU define vários níveis ("tiers") em termos de preparação dos diferentes países, que vale a pena explorar um pouco para podermos identificar melhor qual a situação em que se encontra o espaço lusófono:

Nível 1 (T1) – "Role-modelling": países que obtiveram uma pontuação global [nas métricas definidas pelo Global Cybersecurity Index] de pelo menos 95/100, demonstrando um forte compromisso em matéria de cibersegurança com ações coordenadas e impulsionadas pelos seus governos e que englobam a avaliação, o estabelecimento e a implementação de determinadas medidas de cibersegurança geralmente aceites em todos os cinco pilares, ou até todos.[1]

Nível 2 (T2) – "Advancing": países que obtiveram uma pontuação global de pelo menos 85/100, demonstrando um forte compromisso em matéria de cibersegurança em termos de medidas coordenadas e orientadas pelo governo que abrangem a avaliação, o estabelecimento ou a implementação de determinadas medidas de cibersegurança geralmente aceites em quatro pilares, no máximo, ou um número substancial de indicadores.

Nível 3 (T3) – "Establishing": países que obtiveram uma pontuação global de pelo menos 55/100, demonstrando um compromisso básico de cibersegurança em relação a ações impulsionadas pelos seus governos e que abrangem a avaliação, o estabelecimento ou a implementação de determinadas medidas geralmente aceites num número moderado de pilares ou indicadores.

Nível 4 (T4) – "Evolving": países que obtiveram uma pontuação global de, pelo menos

[1] De acordo com a metodologia da ITU, estes cinco pilares são: Medidas legais; Medidas técnicas; Medidas organizacionais; Medidas de capacidade-desenvolvimento; e Medidas de cooperação.

Foto: PP Creative adobe stock

20/100, demonstrando um compromisso básico em matéria de cibersegurança em relação a ações conduzidas pelo governo que abrangem a avaliação, o estabelecimento ou a implementação de determinadas medidas de cibersegurança geralmente aceites em um pilar, ou vários indicadores e/ou sub-indicadores.

Nível 5 (T5) – "Building": países que obtiveram uma classificação global inferior a 20/100 demonstrando um compromisso básico em matéria de cibersegurança com ações impulsionadas pelo governo que abrangem a avaliação, o estabelecimento ou a implementação de determinadas medidas de cibersegurança geralmente aceites em, pelo menos, um indicador e/ou sub-indicador.

De acordo com este modelo, Portugal e o Brasil surgem como países de Nível 1, mas entre os restantes PALOP, aquele que aparece como tendo maior nível de preparação é Moçambique, no Nível 3.

Investimento e formação

A necessidade de maior investimento – quer ao nível dos Estados, quer das empresas – a par de ações de formação dos cidadãos em geral e dos trabalhadores em particular, parece reunir o consenso entre os responsáveis institucionais e governamentais que estiveram presentes

no recente Fórum Lusófono da Governação da Internet, realizado setembro passado em Maputo (ver caixa "Carta de Maputo").

João Tomar, administrador da ARME (Agência de Regulação Multissectorial da Economia) de Cabo Verde, disse à PTSOC News que a ARME "aconselha as empresas e instituições a investirem no pessoal, a dar-lhes formação, a investir em software de despistagem e de reconhecimento antecipado dos vírus ou das ameaças".

A ARME é a gestora do domínio .CV bem como da infraestrutura de chaves públicas do país. João Tomar indicou que o governo de Cabo Verde "adotou o digital como política pública, como um investimento prioritário", até como forma de captar investimentos para instalação de centros de dados e atração de nómadas digitais.

Para estes projetos, Cabo Verde tem contado também com investimentos do Banco Mundial. "No mundo digital de hoje, sem confiança, sem segurança, não há negócio", conclui João Tomar.

Phishing e ransomware

O vetor de ataque mais comum, transversal a todos os países da Lusofonia, é o phishing, em muitos casos associado ao ransomware.

O Professor Lourino Chemane, presidente do conselho de administração do INTIC

Carta de Maputo

Os organizadores do 3.º Fórum Lusófono da Governação da Internet aprovaram um documento final, a "Carta de Maputo", no qual "convidam os países lusófonos e as suas ativas comunidades a mobilizarem os setores da sociedade civil, da comunidade técnica, dos pesquisadores nas academias em inúmeras áreas de conhecimento, dos setores empresariais que desenvolvem, produzem, comercializam e utilizam a Internet e serviços digitais para com os seus respetivos governos em todas as suas esferas a debaterem, em processos consensuais multissetoriais, propostas de regulação sobre uso das plataformas sociais, sobre a inteligência artificial, sobre segurança cibernética, sobre proteção da privacidade dos dados pessoais, sobre governança digital."

Além disso, o documento reconhece que "a capacitação sobre Governação da Internet entre os países lusófonos será primordial para a consolidação de modelos fundados nos princípios multissetoriais, incluindo temas globais como, nomeadamente, a inteligência artificial, a cibersegurança, a proteção de dados pessoais, a governação de dados, abrangendo visão sistémica para a construção de um ecossistema lusófono mais resiliente, seguro e de confiança. Intercâmbios entre os Fóruns Locais e Programas de Jovens no ecossistema de governação Lusófona da Internet serão relevantes contributos."

O documento completo pode ser consultado em https://igf-lusofonia.pt/carta-de-maputo.

Foto: Delta Amphule, adobe stock

– Instituto Nacional de Tecnologias de Informação e Comunicação de Moçambique, identifica o phishing como o principal vetor de ataque em Moçambique, "visando principalmente aos meios de pagamento eletrónico acedidos através da Internet, providos pela banca e maioritariamente nos centros urbanos", assim como as carteiras móveis fornecidas pelos operadores de telecomunicações. Este é um alvo que abrange toda a população nos locais onde há cobertura de telecomunicações, incluindo as zonas rurais, onde a cobertura atual é cerca de 19 milhões de utilizadores.

Este responsável destaca também as "burlas que envolvem pessoas pedindo dinheiro via SMS, WhatsApp e redes sociais", bem como o phishing através de email, telefone ou outros meios de telecomunicação "para que cedam dados, senhas, façam transferências ou cliquem em links maliciosos".

Também André Pedro, diretor do INFOSI – Instituto Nacional de Fomento da Sociedade da Informação, de Angola, confirma que "o phishing é o líder de todos [os vetores de ciberataques]" no país, e identifica as redes sociais como uma das principais fontes destas ameaças. São mensagens, explica, "voltadas para os utilizadores finais, do tipo 'atualiza a tua conta que a gente ajuda' ou 'se tiveres dificuldade a receber recibos…'".

Já Rodolfo Avelino, Conselheiro do Comitê Gestor da Internet no Brasil, admite que há

Projeto de Capacitação Digital

A LusNIC, associação que agrega todos os gestores de domínios de topo da lusofonia, em parceria com a Coalition for Digital Africa da ICANN, está a desenvolver um projeto de capacitação digital destinado aos ccTLDs africanos seus membros (.cv, .ao, .st, .gw e .mz). A iniciativa decorre até março de 2026 e representa um passo estratégico na consolidação das capacidades técnicas, jurídicas e operacionais destes registries.

Segundo Marta Moreira Dias, presidente da LusNIC e vogal do Conselho Diretivo do .PT, "o apoio e colaboração com os congéneres da lusofonia, tem sido desde sempre uma prioridade do .PT, não só enquanto membro fundador da LusNIC mas também na sua qualidade de responsável pelo ccTLD nacional, trabalhando diariamente para a construção de um espaço digital lusófono mais aberto, transparente, seguro e resiliente."

Este projeto em particular prevê ações formativas online e presenciais, baseadas num levantamento específico das necessidades de formação de cada ccTLD visado, a construção de planos de negócio adaptados à realidade de cada país, e a tradução de materiais de referência para português.

O primeiro momento formativo foi realizado no dia 24 de setembro em Moçambique, integrado na programação do Fórum Lusófono da Governação da Internet, e consistiu em cinco painéis que contaram com a participação de seis formadores do .PT.

No total, o projeto contempla quatro ações de formação, duas presenciais e duas online, que irão decorrer até fevereiro de 2026. Cada sessão será adaptada às realidades e prioridades de cada país, garantindo impacto prático e alinhamento com os objetivos de desenvolvimento digital da região.

Foto: hdesert, adobe stock

muitos incidentes que acabam por não ser reportados, "mas dos reportes que temos, os de ransomware acabam por ser os mais comuns, sendo que em muitos deles o vetor de ataque é também o phishing – um e-mail ou algum outro tipo de interação do utilizador."

De acordo com estes três responsáveis, em qualquer dos países, a forma de mitigar estes tipos de ataques e ameaças passa, em grande parte, pelo investimento em ações de formação promovidas pelas instituições responsáveis, tendo como alvos utilizadores finais e empresas.

Lourino Chemane salienta também os esforços do seu governo no sentido de aumentar a resiliência digital do país, nomeadamente através de investimentos realizados com a criação de quadros legislativos e regulamentares robustos bem como melhorias na interoperabilidade entre entidades públicas, sector privado, academia e sociedade civil, entre outras medidas.

Portugal: incidentes crescem 36%

Em Portugal, o Centro Nacional de Cibersegurança (CNCS) acaba de publicar a 6.ª edição do seu relatório Riscos e Conflitos, no qual se revela um aumento de 36% no número de incidentes relacionados com cibersegurança em 2024, face ao ano anterior.

Lino Santos, coordenador do CNCS e também presente no evento de Maputo, confirma que as principais preocupações "dizem respeito aos esquemas de phishing associados a burlas de todo o tipo; ou seja, instrumentos de engenharia social perpetrados por agentes de cibercrime organizado."

No entanto, é também preocupante "aquilo que são os furtos de identidade e furtos de dados pessoais que decorrem de um fenómeno chamado 'Info Stealer', um tipo de malware muito comum que afeta maioritariamente dispositivos móveis, mas também computadores, e que exfiltra tudo o que tem a ver com dados pessoais dos nossos acessos aos sistemas de home banking, às nossas contas de correio eletrónico, notas de uso pessoal ou de uso profissional, mas também o nosso perfil de utilização de redes sociais e de browsers. No fundo, toda a nossa pegada digital exfiltrada por estes criminosos que depois é criada, quantificada e amortizada na Dark Web."

"E isto preocupa-nos, primeiro pela própria quebra de dados de proteção de dados pessoais, mas também porque este aumento é um passo e um instrumento importante para a realização de outras tipologias de ataques, como por exemplo ransomware, utilizando credenciais válidas, adquiridas na Dark Web, como forma de entrada ou de primeira entrada na infraestrutura das organizações", explica.

O papel dos administradores de servidores DNS

José Casinha, Vogal do Conselho Diretivo Executivo do .PT, defende que os administradores de servidores DNS devem desempenhar "um papel crucial na redução dos riscos associados a ataques como *phishing, smishing* e *pharming*, devendo implementar mecanismos técnicos e operacionais que reforcem a integridade e a resiliência do sistema."

"Entre as medidas prioritárias destaca-se a implementação do DNSSEC, que assegura a autenticidade das respostas DNS e previne redirecionamentos maliciosos", explica este responsável. "É igualmente recomendável o uso de DNS sobre TLS (DoT) e DNS sobre HTTPS (DoH), para proteger a confidencialidade e integridade das consultas. A aplicação de políticas como *rate limiting* e *Response Policy Zones* (RPZ) permite bloquear domínios maliciosos e reduzir o impacto de ataques de amplificação."

Para José Casinha, "a higiene dos registos DNS é essencial: devem ser monitorizadas alterações não autorizadas, restringidos os acessos administrativos com autenticação multifator e garantidos logs de auditoria. No combate ao phishing por email, é fundamental configurar e monitorizar SPF, DKIM e DMARC, prevenindo o uso fraudulento dos domínios."

Além disso, "os servidores devem ser segmentados e isolados, com controlos rigorosos de transferência de zonas e mecanismos de backup e recuperação testados. A monitorização contínua do tráfego DNS, apoiada em *feeds* de *threat intelligence*, permite detetar padrões anómalos e domínios suspeitos em tempo real."

"Por fim, a segurança do DNS deve ser complementada com formação das equipas e vigilância ativa da reputação dos domínios, garantindo uma defesa abrangente contra tentativas de manipulação e fraude digital", conclui José Casinha.

3

António Ribeiro

Head of Cybersecurity na Minsait em Portugal (Indra Group)

1. A maioria dos problemas/desafios em termos de cibersegurança é transversal. No caso dos PALOP, existem desafios específicos em cada país?

Apesar das diferenças entre os países, os PALOP enfrentam desafios comuns em matéria de cibersegurança. As infraestruturas tecnológicas são, em muitos casos, frágeis ou desatualizadas, o que limita a capacidade de resposta a incidentes. O investimento em segurança digital continua a ser reduzido, refletindo-se na escassez de ferramentas adequadas e na ausência de estratégias nacionais robustas. A falta de profissionais qualificados, aliada à inexistência de programas de formação contínua, agrava a vulnerabilidade das organizações. Além disso, a baixa literacia digital e a limitada sensibilização da população para os riscos cibernéticos tornam o fator humano um dos principais vetores de risco.

Paralelamente, cada país apresenta as suas próprias especificidades: Angola regista um elevado número de ataques, sobretudo nos setores da educação e saúde. Estima-se que o país sofra mais de 250 tentativas de intrusão por dia, com destaque para ataques de ransomware e phishing; Moçambique lidera nos PALOP, no nível de maturidade em cibersegurança, segundo o relatório da União Internacional das Telecomunicações (UIT) publicado em setembro de 2024; Cabo Verde, tem feito progressos significativos, com a criação da Agência Nacional de Comunicações e da Estratégia Nacional de Cibersegurança, no entanto, precisa de reforçar a resiliência digital; e a Guiné-Bissau e São Tomé e Príncipe apresentam os níveis mais baixos de preparação, com recursos limitados e elevada exposição a ameaças. Estes contextos reforçam a necessidade de estratégias adaptadas, e investimento em capacidades locais e cooperação regional.

A nível da cooperação regional, o continente africano ainda não beneficia de uma entidade de coordenação global, com capacidade de definir políticas, regular, certificar e coordenar a cooperação entre os diversos estados, à semelhança do que existe a nível

europeu com a Enisa. Alguns esforços estão a ser feitos nesse sentido com a certeza de que os PALOPs irão beneficiar bastante desta cooperação.

2. Muitos problemas de cibersegurança podem ser mitigados com investimento adequado em medidas concretas (hardware/software/formação…). Até que ponto empresas e instituições em economias mais frágeis estão, também por isso, mais vulneráveis a ameaças de cibersegurança?

A cibersegurança é, hoje, um dos pilares fundamentais da resiliência digital das organizações. No entanto, em economias mais frágeis, a limitação de recursos financeiros e humanos pode dificultar o investimento consistente em medidas essenciais como infraestrutura tecnológica robusta, software atualizado e, sobretudo, formação contínua das equipas. Esta realidade torna estas organizações mais vulneráveis a ciberataques, que exploram precisamente as suas fragilidades.

Nos PALOP, embora se observem sinais positivos o desafio do desenvolvimento de capacidades técnicas e humanas continua a ser crítico para a maioria dos países da região. É neste contexto que adaptamos a nossa resposta aos desafios de segurança de cada organização, sector e nível de maturidade. Empresas com presença internacional e experiência em ambientes de maturidade digital variável, como é o caso da Minsait, têm procurado apoiar estas economias com abordagens que combinam tecnologia, serviços geridos e formação contínua. O objetivo é claro: garantir que a proteção digital não seja um privilégio, mas uma base acessível para o desenvolvimento sustentável e seguro."

3. Nos últimos anos, o ransomware tem vindo a posicionar-se como um dos principais problemas em termos de cibersegurança, com a agravante de que muitos dos vetores de ataque têm origem em "engenharia social". O fator humano – e, neste caso concreto, a formação dos trabalhadores – é algo que poderá constituir um maior desafio nestas regiões, face ao que já se verifica nos países ocidentais?

O fator humano continua a ser, indiscutivelmente, a primeira linha de defesa de uma organização. O crescimento exponencial dos ataques de ransomware, frequentemente iniciados por técnicas de engenharia social como o phishing, reforça a importância da formação contínua e da consciencialização dos colaboradores das várias organizações e da população no geral.

A engenharia social para ser bem-sucedida tem, por um lado, de ser enquadrada no contexto específico do alvo, e por outro, o alvo tem de ser apelativo para o atacante, seja por motivos financeiros ou por quaisquer outros. Neste sentido há, neste campo, uma dupla ação cometida pelos criminosos, primeiro

Foto: Rocha Santos, adobe stock

ao atuarem no seu mercado original, mas também, como temos visto, ao exportarem esta engenharia social para mercados mais apelativos, como seja o mercado europeu.

Nos PALOP, este desafio é percetível. A escassez de profissionais mais qualificados, a limitada oferta de programas de formação técnica especializada e os baixos níveis médios de literacia digital dificultam a criação de uma cultura de cibersegurança sólida. Embora faltem dados consolidados para todos os países da região, sabe-se que a maioria ainda enfrenta dificuldades estruturais no acesso à educação digital e à capacitação técnica, o que amplia a vulnerabilidade a ataques baseados em engenharia social.

Apesar disso, há sinais de progresso. Iniciativas de capacitação promovidas por universidades, organizações multilaterais e empresas tecnológicas têm vindo a ganhar tração. É neste contexto que soluções de cibersegurança que integram não apenas tecnologia, mas também componentes de formação e sensibilização, assumem um papel estratégico. Empresas com experiência em ambientes de maturidade digital variável, como a Minsait, têm procurado apoiar estas regiões com abordagens que valorizam a transferência de conhecimento e o reforço das competências locais.

A melhor tecnologia do mundo será sempre insuficiente se os utilizadores não estiverem preparados para reconhecer e evitar as ameaças mais comuns. E é precisamente aí que reside o maior desafio – e também a maior oportunidade – para os PALOP.

Mês Europeu da Cibersegurança: #THINKB4UCLICK

"Think Before U Click" (Pense Antes de Clicar) é, desde 2020, o mote do "Mês Europeu da Cibersegurança" (ECSM), uma iniciativa da Agência da União Europeia para a Cibersegurança (ENISA) e da Comissão Europeia, que em Portugal conta com a coordenação do Centro Nacional de Cibersegurança (CNCS).

A ideia desta campanha anual, que cumpre este ano a sua 13.ª edição, é promover a cibersegurança entre os cidadãos e as organizações da União Europeia (UE) e fornecer informações atualizadas sobre segurança online através da sensibilização e da partilha de boas práticas.

Todos os anos, durante todo o mês de outubro, realizam-se centenas de atividades em toda a Europa, incluindo conferências, workshops, formações, webinars e apresentações, entre outras, para promover a segurança digital e a ciber-higiene, sobretudo ao nível dos cidadãos da UE.

Em 2025, a ENISA continua a assumir o papel de coordenadora da organização da campanha, atuando como um "hub" para todos os Estados-Membros e instituições da UE participantes e fornecendo sugestões de peritos, gerando sinergias e promovendo mensagens comuns entre os cidadãos, as empresas e a administração pública da UE.

O crescimento do phishing – um espinho no meu (web)site

Segundo a ENISA, o phishing continua a ser o principal vetor de intrusão inicial, sendo responsável por cerca de 60% dos casos, continuando a ser uma técnica eficaz para efetuar ciberataques.

O phishing pode ocorrer de muitas formas, como a implementação de falsos avisos CAPTCHA em websites comprometidos ou fraudulentos, que induzem os utilizadores a executar comandos sob o pretexto de verificação humana.

Além disso, as plataformas de "Phishing-as-a-Service", concebidas para automatizar a geração de kits de phishing através da clonagem de páginas de início de sessão e da distribuição de ligações, permitiram aos cibercriminosos e a outros agentes de ciberameaças imitar empresas e marcas de confiança e enganar os utilizadores.

Pior, começou a generalizar-se a utilização de ferramentas de IA, através de LLMs, para criar emails de phishing mais convincentes. No início de 2025, as campanhas de phishing apoiadas por IA representavam mais de 80 por cento da atividade de engenharia social observada em todo o mundo.

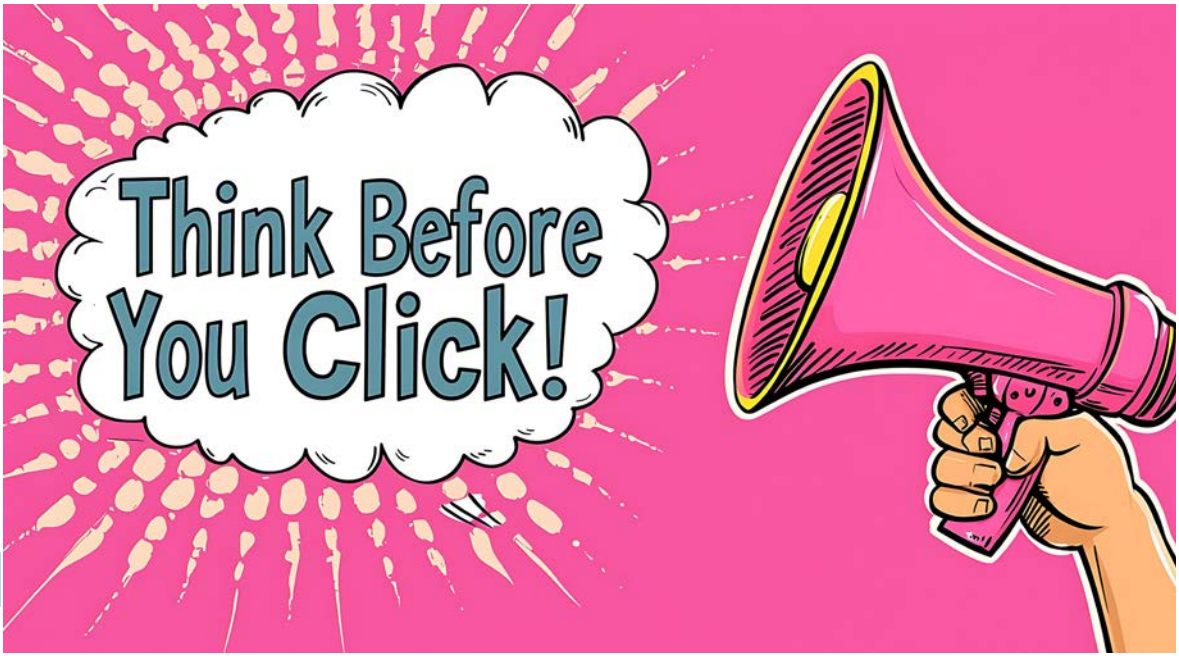

Foto: A2Z AI, adobe stock

Daí que a ENISA tenha aproveitado as iniciativas deste mês de outubro para "apelar a todos os utilizadores para que estejam conscientes da variedade de phishing e ciberfraudes que existem", incluindo:

- Phishing - phishing baseado em email
- Quishing - phishing com código QR
- Spearphishing - phishing direcionado
- Smishing - phishing de texto SMS
- Vishing - phishing baseado na voz
- Whaling - phishing de liderança de topo
- BEC - esquemas de comprometimento do email empresarial
- Deepfakes - fraudes baseadas em IA

Como em anos anteriores, este mês voltou a ser assinalado por diversas iniciativas e publicação de estudos que se irão manter acessíveis e constituem uma excelente fonte de informação e prevenção na área da cibersegurança.

Apesar de não ser algo dependente do ECSM, vale a pena salientar que o CNSC oferece diversos cursos gratuitos no formato e-learning que permitem aos cidadãos adquirirem competências que os tornem mais informados e, consequentemente, resilientes perante ciberameaças – quer no seu dia-a-dia, quer no contexto das empresas em que trabalham.

Trata-se de cursos disponíveis na plataforma NAU que abordam vários temas, nomeadamente sobre ciber-higiene, desinformação, compras online e segurança no contexto das redes sociais. Todos estes quatro cursos encontram-se disponíveis gratuitamente até ao dia 18 de dezembro de 2025.

ENISA Threat Landscape October 2025

O mais recente relatório de ameaças da ENISA para 2025 mostra que os grupos de ameaças estão a reutilizar ferramentas e técnicas, a introduzir novos modelos de ataque, a explorar vulnerabilidades e a colaborar para afetar a segurança e a resiliência das infraestruturas digitais da UE.

Através de uma abordagem mais centrada nas ameaças e de uma análise contextual mais aprofundada, este estudo analisou 4875 incidentes entre 1 de julho de 2024 e 30 de junho de 2025.

Eis alguns dos destaques da ENISA sobre o cenário de ameaças em 2025:

- O ransomware é identificado como a ameaça com maior impacto na UE;
- O chamado 'hacktivismo' assumiu a liderança, representando quase 80% do número total de incidentes, principalmente através de campanhas DDoS de baixo impacto dirigidas a sítios Web de organizações dos Estados-Membros da UE, sendo que apenas 2% dos incidentes de hacktivismo resultaram em perturbações do serviço;
- Os grupos de ameaça alinhados com o Estado intensificaram constantemente as suas operações contra organizações da UE. Os agentes do Estado em situação de "anexo" levaram a cabo ciberespionagem contra o sector da administração pública, enquanto o público da UE foi confrontado com a Manipulação e Interferência de Informação Estrangeira (FIMI);
- O phishing (60%), seguido da exploração de vulnerabilidades (21,3%), são os dois principais pontos de acesso à intrusão.

Relatório Riscos e Conflitos 2025

O Centro Nacional de Cibersegurança divulgou no final de Setembro a **6.ª edição do Relatório Riscos e Conflitos**, no qual se releva que, em 2024, o número de incidentes de cibersegurança "aumentou significativamente, num ano marcado por uma elevada incidência de ataques de phishing e smishing, outras formas de engenharia social, pela exploração de vulnerabilidades, negação de serviços distribuída (DDoS) e, pelo seu impacto, o ransomware"

De acordo com o documento, "os incidentes mais relevantes de 2024 foram sobretudo relacionados com código malicioso no seu sentido mais lato, destacando-se os casos de ransomware e de infostealers que impactaram o país, num ano caracterizado por vários leaks de credenciais."

QUADRO DE AMEAÇAS: CIBERAMEAÇAS/AGENTES DE AMEAÇA CRÍTICOS EM PORTUGAL, 2024/2025

TOP 10 - Ciberameaças/ TOP 3 - Agentes de ameaça	Cibercriminosos	Agentes Estatais	Hacktivistas
Phishing e *Smishing*			
Engenharia Social e Burlas *Online*			
Ransomware			
Exploração de Vulnerabilidades			
Negação de Serviço Distribuída (DDoS)			
Comprometimento de Contas			
Código Malicioso			
Exfiltração de informação			
Ciberespionagem			
Tentativa de *Login*			

Agentes de ameaça e ciberameaças com relevância elevada em Portugal durante 2023/2024.
Agentes de ameaça e ciberameaças com relevância média em Portugal durante 2023/2024.
Ciberameaça com frequência elevada como prática dos agentes de ameaça em causa em Portugal.
Ciberameaça com frequência média como prática dos agentes de ameaça em causa em Portugal.
Ciberameaça com frequência baixa ou inexistente como prática dos agentes de ameaça em causa em Portugal.

Fonte: CNCS

State of AI in Telecommunications: 2025 Trends

A Nvidia divulgou o seu terceiro relatório anual sobre o "Estado da IA nas Telecomunicações", o qual "revelou que 97% dos inquiridos do sector das telecomunicações estão a avaliar ou a adotar a IA com o objetivo de melhorar as experiências dos clientes e produtividade dos funcionários, melhorar as operações de rede, reduzir custos e abrir novas oportunidades de negócio."

Os inquiridos dividem-se em termos de implementação e avaliação ativas da IA, com 49% a utilizá-la ativamente e outros 49% numa fase de avaliação de ensaios ou projectos-piloto. Os inquiridos que afirmaram *não estar* a utilizar ou a planear utilizar a IA diminuíram de 10 por cento no inquérito de 2023 para apenas 3 por cento em 2024.

The State of Broadband in Africa

A ITU, agência da ONU para as tecnologias digitais, divulgou em setembro um relatório intitulado The State of Broadband in Africa (O Estado da Banda Larga em África), no qual, entre outros, se faz um ponto de situação e salientam os avanços do continente em termos de cobertura celular.

Enquanto que em países onde a cobertura celular começou há mais anos não existe desde há muito redes 2G e as redes 3G começam a ser desligadas, de acordo com este estudo, no final de 2024, pouco mais de metade de todas as ligações móveis no continente eram ainda 3G e 10% dos utilizadores continuavam a utilizar 2G.

Ainda assim, a cobertura 4G cresceu para um terço de todas as ligações. Espera-se que a utilização do 3G diminua à medida que o 4G se expande, mas projeta-se que a cobertura 5G atinja apenas 17% de penetração até 2030.

Organização

.pt

CURSO

Cód. GRCO

Gestão dos Riscos de Cibersegurança nas Organizações

Salvaguarde a integridade da sua organização identificando vulnerabilidades e planeando estratégias de mitigação em caso de ciberataque.

Descrição

Com a crescente digitalização dos serviços e negócios, cresce o risco de ciberataque e de comprometimento das operações vitais das organizações. O curso “Gestão dos Riscos de Cibersegurança nas organizações” aborda o processo de identificação, avaliação e tratamento de riscos de cibersegurança nas organizações.

Nos primeiros módulos, apresenta-se em detalhe o processo de análise e gestão de risco e, no último módulo, o formando terá de por à prova os seus conhecimentos respondendo a exercícios de aplicação.

Formato

- Duração: 10 horas
- Esforço: 10 horas
- Ritmo: Ao ritmo do estudante
- Idiomas: Português

Curso

Disponível até 05/06/2026

Curso através da plataforma nau SEMPRE A APRENDER

Mais informações em
www.nau.edu.pt

Organização

.pt

CURSO

Cód. CNCIS

Gestão da Continuidade de Negócio

O que deve uma organização fazer quando um evento interrompe a normal entrega de bens ou serviços?

Descrição

Atualmente, os ciberataques são uma ameaça constante, tanto a pessoas individuais como a organizações. As organizações devem identificar as potenciais ameaças às operações críticas, bem como os impactos que poderão surgir caso estas ameaças se materializem.

As organizações necessitam de proteger as atividades vitais, definindo uma estratégia e elaborando o Plano de Continuidade de Negócio. Os procedimentos que a organização venha a definir devem ser testados e revistos. Neste curso terá a oportunidade de aprender os conceitos básicos de gestão da continuidade de negócio bem como de aplicar os conhecimentos desenvolvidos através de um caso prático.

Formato

- Duração: 10 horas
- Esforço: 10 horas
- Ritmo: Ao ritmo do estudante
- Idiomas: Português

Curso

Disponível até 02/04/2026

Curso através da plataforma nau SEMPRE A APRENDER

Mais informações em
www.nau.edu.pt

Esta publicação é produzida pelo .PT

Editor
António Eduardo Marques

Design Gráfico
Sara Dias
Maria Cristóvão

Fotografia
Capa: smalltinykid, adobe stock
Índice e contracapa: Jason Yoder, adobe stock

Publicação trimestral
Outubro 2025


.pt
www.pt.pt