EDIÇÃO Nº 1 | REVISTA DIGITAL TRIMESTRAL | JUNHO 2025

digiangolê

Cibersegurança, blockchain, fintechs e remessas

— Tudo o que você precisa saber para estar preparado.

Entrevista exclusiva com

Diretora de Marketing da KWATTEL

kwattel.com

Informação. Conexão.
Tudo Digital.

FICHA TÉCNICA

Revista DigiAngolê

Edição Nº1: Junho 2025 (Trimestral)

Direção da Publicação: Coimbra Adolfo “Matadi”

Edição Digital: Joel Sales

Realização: ABV

Coordenação Científica: Iguana Comunicações

Design Gráfico: Daniela Gonçalves (Portugal)

Textos da Edição Nº1: Joel Sales, Dulce Janaína, Edmilson Junior, Adérito Veloso, Plácida Savo, Sebastian Rafael, Conceição Inglês

Sumário

Editorial

A revista DigiAngolê, de edição trimestral, é uma publicação digital do grupo IGUANA COMUNICAÇÕES, criada dois anos após o lançamento da rádio FM Afro.

Este será um espaço dedicado à divulgação de opiniões sobre as mais inovadoras tecnologias de pagamento e sobre políticas de inclusão financeira, ações fundamentais numa sociedade em que tais estratégias são essenciais para reduzir os índices de exclusão social e formalizar os movimentos de pagamento e serviços digitais. Esse processo visa tornar o sistema mais eficiente e acessível aos cerca de 50% da população que ainda está fora do sistema bancário.

A revista também servirá como plataforma para que os nossos colaboradores e convidados compartilhem visões inovadoras e proponham soluções para os desafios do mercado de carteiras digitais.

Nesta primeira edição, o tema central é a problemática da Cibersegurança, abordada por meio de textos curtos, mas densos em substância. Em segundo plano, destacamos uma grande entrevista com a diretora de marketing da KWATTEL, além de uma análise instigante sobre remessas internacionais, feita por um analista de origem tanzaniana, país com um mercado de Mobile Money bastante maduro.

Os textos de opinião não vinculam o editor, são textos que traduzirão a cultura da pluralidade.

Joel Sales
Direção da Publicação

Cibersegurança

Necessidade de investimento em Cibersegurança em Angola

Autora: Dulce Janaína
Ciência da Computação e Ciber Segurança

Atualmente, Angola é um dos países africanos que mais sofrem ataques cibernéticos. De acordo com o "Data Group" [1] em 2021 Angola foi um dos países mais afetados por ataques cibernéticos no mundo. Em 2022, uma pesquisa da Cloudflare [2] apontou a Angola como o segundo país africano e quarto país no mundo que mais sofreu ataques de negação de serviço.

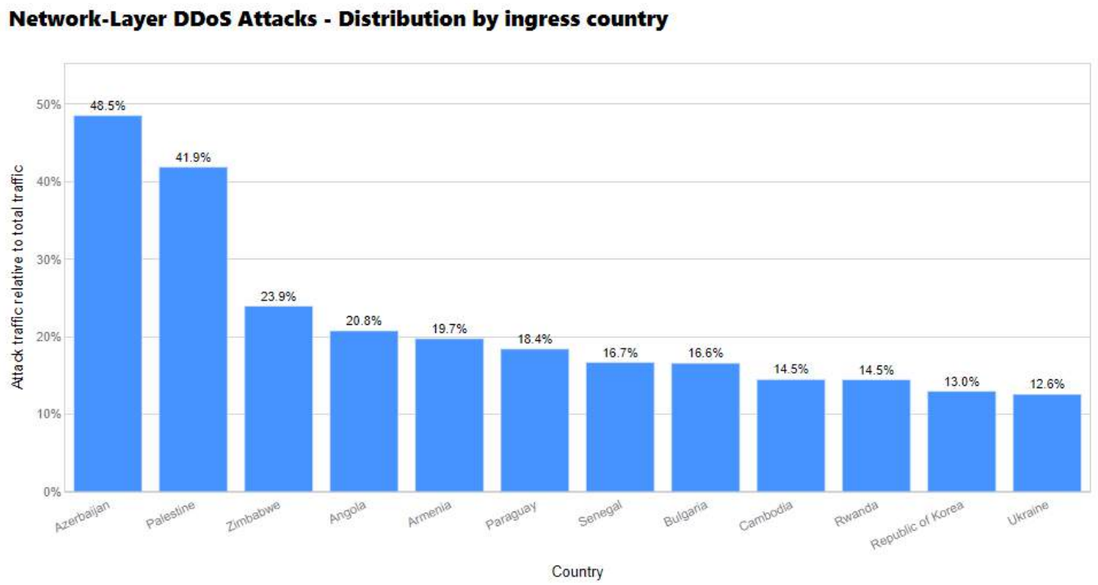


Fig. 1: Porcentagem de tráfego malicioso em relação ao total de tráfego registrado (Fonte: Cloudflare [2])

No ano de 2024, milhares de ataques cibernéticos foram registrados no país, onde a maioria destes ataques são direcionados ao setor de Internet e Telecomunicações (70,69%), seguido pelo setor de Serviços (18.83%) e Tecnologia (4.18%).

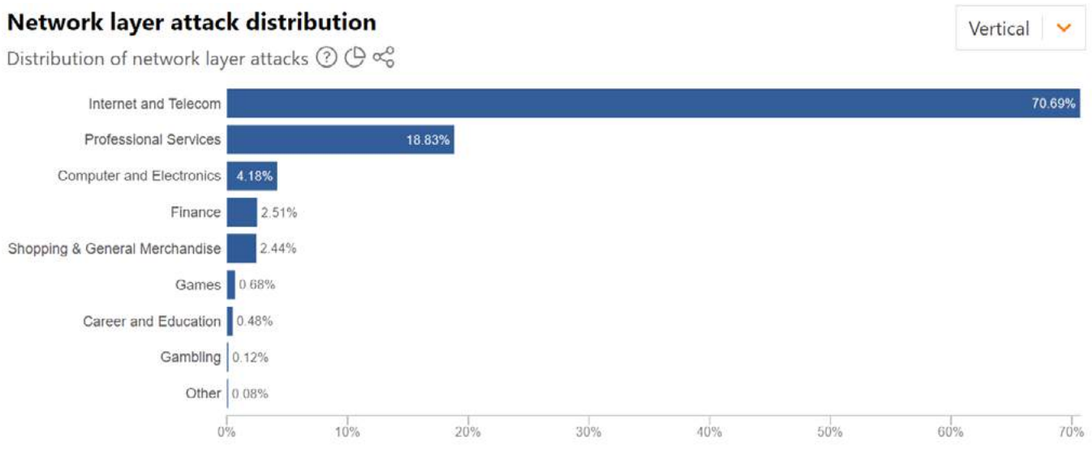


Fig. 2: Setores mais afetados por ataques Cibernéticos (Fonte: Cloudflare [3])

Grandes incidentes de segurança vêm se tornando cada vez mais comuns em Angola. Em 2019, a Sonangol sofreu um incidente de cibersegurança que afetou as operações da empresa causando danos financeiros [4]. No início de 2024, o Banco Nacional de Angola (BNA) sofreu um ataque de Ransomware que comprometeu bases de dados e serviços do banco [5]. No mês de setembro, a Transportadora aérea angolana (TAAG) sofreu um ataque cibernético, com consequências ainda não divulgadas pela TAAG [6]. Estes ataques mostram como grandes instituições angolanas são bastante visadas por atores maliciosos e como a complexidade dos ataques vem evoluindo nos últimos anos.

Para mitigar e reduzir o impacto desses ataques, o governo angolano, através do Ministério das Telecomunicações, Tecnologias de Informação e Comunicação Social (MINTTICS), criou o projecto estruturante de Infra-estrutura de Cibersegurança [7]. Este projeto almeja atender a necessidade de um centro para auxiliar no tratamento, resolução e resposta de incidentes informáticos. Outra iniciativa importante do governo é a participação no African Joint Operation Against Cybercrime (AFJOC), projeto de cibersegurança da Interpol para o continente africano que permite que os países membros partilhem experiências no combate a o cibercrime.

Apesar das medidas de cooperação criadas pelo governo, ainda existem diversas oportunidades para melhorar o ecossistema de segurança cibernética angolano. O projecto estruturante de Infra-estrutura de Cibersegurança pode evoluir para um Centro de Estudos, Resposta e Tratamento de Incidentes, capaz de estabelecer recomendações e diretrizes sobre preservação de evidências digitais e resposta a incidentes informáticos. Governo e empresas angolanas também podem compartilhar entre si informações referentes a ataques cibernéticos para auxiliar na investigação e prevenção de ataques futuros.

Por fim, é de máxima importância investir na capacitação, formação e retenção de pessoal capacitado em segurança cibernética. A demanda por profissionais da área aumenta cada vez mais todos os anos e a fuga de talentos para países e empresas estrangeiras em busca de melhores condições de trabalho podem ocasionar uma falta de mão de obra qualificada em um futuro de médio prazo. É importante lembrar que a segurança da informação se baseia em três pilares fundamentais: Pessoas, Processos e Tecnologia.

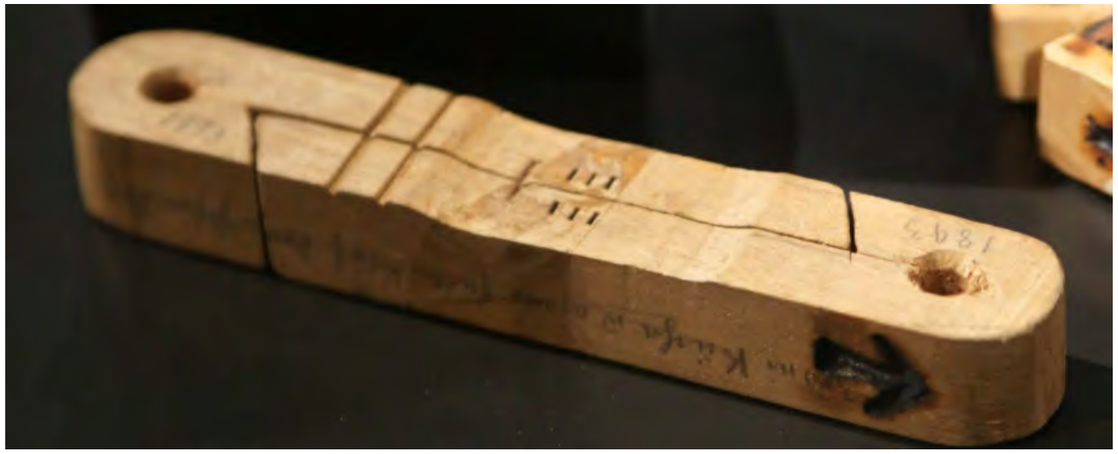
O desafio das empresas angolanas nos próximos anos será manter pessoal capacitado para a defesa dos seus ambientes informáticos. Porém, também será necessário investir em processos e tecnologias efetivas para defender os ambientes de infraestrutura crítica de atores maliciosos.

Tecnologia Blockchain e Tokenização de ativos

Autor: Edmilson Rodrigues do Nascimento Junior
Mestre em Ciências da Computação (UFPE)

Desde que as sociedades humanas desenvolveram o conceito de propriedade privada surgiu um problema: Como ter certeza de que alguma coisa pertence a alguém em determinado momento? E se alguma coisa, por exemplo um pedaço de terra, for vendida, como o resto da sociedade vai saber que a propriedade mudou de dono?

Estudiosos afirmam que a escrita cuneiforme dos Sumérios, que eram feitas a partir de marcações em tabletes de argila, foi criada para manter registros dos grãos pagos (os primeiros impostos). Já os ingleses da era medieval usavam uma tecnologia baseada em pedaços de madeiras cravados chamados “Tallies” .



Com o advento dos computadores e da era da informação, a maior parte dos registros de transações passou a ser feita através de sistemas de informações que eram gerenciados por Bancos. Os bancos, por sua vez, eram supervisionados por instituições nacionais e supranacionais (como a Basiléia). Mas isso trouxe um novo problema: Agora as pessoas precisam confiar nos bancos, nos governos e nas instituições supranacionais. E como demonstra a grande crise do Subprime dos EUA em 2008, nem sempre essas instituições estão à prova de erro, nem têm o interesse do cidadão médio como prioridade.

Não por coincidência, foi também em 2008 que surgiu uma nova tecnologia chamada de Blockchain, que é a base do Bitcoin. É um sistema de registro digital distribuído e imutável, onde as transações são registradas em blocos interligados e criptografados, garantindo segurança e transparência.

A partir de origens humildes, em que foi proposta através de um fórum sobre criptografia o “whitepaper” do Bitcoin. A tecnologia do blockchain teve uma “explosão cambriana” de inovação, e não demorou muito para as pessoas perceberem que a verdadeira inovação estava na tecnologia do Blockchain.

Hoje as criptomoedas criadas a partir de inovações com essa tecnologia somam um mercado de $2.2 trilhões de dólares, segundo o CoinMarket Cap.

A tecnologia Blockchain é uma coisa tão especial por que oferece segurança e transparência para transações, tornando-as mais confiáveis e rastreáveis. Hoje, está sendo apropriada até por governos para a criação das chamadas CBDCs (Central Bank Digital Currencies). E a tecnologia vem sendo adotada em diversas áreas, como saúde, logística e governança. Em particular, a tecnologia blockchain vem influenciando a indústria bancária e de pagamentos pela promessa de custos reduzidos, pagamentos mais rápidos, e maior transparência e segurança.

Uma empresa que utiliza a tecnologia Blockchain para modernizar a infra-estrutura de bancos e empresas de pagamentos é a Ripple (https://ripple.com/). Através de seus produtos, empresas de diversos países usam suas soluções para facilitar pagamentos transnacionais e ter acesso a uma “stablecoin” lastreada no dólar. Outra empresa que desenvolveu alternativas Open Source de stablecoins é a Mento Labs (https://www.mentolabs.xyz/), cujas stablecoins denominadas em dólar, euro e outras moedas são usadas em diversos países.

As “stablecoins” são um exemplo de “tokenização de um ativo, que consiste em se transformar um ativo do mundo real, como a moeda de um país, um crédito de carbono, um título de terra, a propriedade de uma casa, ações de uma empresa, obras de arte, etc... em um “token”, ou seja, um registro único em uma blockchain. Nesse processo que surge o conceito de “tokenização de ativos”.

Dentre os principais benefícios de tokenizar-se um ativo estão:

1) Fracionamento de propriedade: Permite a propriedade fracionada de ativos, tornando-os acessíveis a um público mais amplo.

2) Transferência instantânea e global: A Blockchain possibilita transferências globais de propriedade de forma instantânea e segura.

3) Aumento da liquidez: A tokenização aumenta a liquidez dos ativos pois mais pessoas em diferentes lugares podem participar da negociação daquele ativo.

Além do caso de uso do setor bancário e de pagamentos, pode-se mencionar alguns casos de uso e empresas que já atuam na tokenização de diversos ativos, como:

Imóveis: A tokenização permite a compra e venda de imóveis de forma rápida e eficiente, além de facilitar o financiamento e a divisão de propriedades. Um exemplo de empresa fazendo isso no Brasil é a Nestpaces, cujo site é: https://www.netspaces.org/

Artes e artigos de luxo: Obras de arte ou artigos de luxo podem ser tokenizados, tornando-as mais acessíveis e facilitando sua comercialização.

Cadeia de suprimentos: A tokenização pode ser utilizada para rastrear produtos ao longo de toda a cadeia de suprimentos, garantindo sua autenticidade e origem. Esse é o caso da empresa alemã “LoopID” que cria uma espécie de passaporte virtual de cada produto. Vide o site: https://www.loopid.com/

Comércio: A tokenização pode ser utilizada para facilitar transações comerciais, com pagamentos seguros e transparentes. Esse é o caso da empresa Alemã Mento Labs (https://www.mentolabs.xyz/) que faz a tokenização de artigos, desde dinheiro a créditos de carbono.

Sendo assim, a tecnologia Blockchain e a tokenização de ativos estão transformando a forma como as pessoas interagem com os ativos, abrindo um leque de novas oportunidades para diversos setores. E um dos setores que espera-se será mais afetado quando essa tecnologia se popularizar é o setor bancário e de pagamentos. Não à toa países ao redor do mundo estão investindo na adaptação da tecnologia blockchain para modernizar seus sistemas de pagamentos.

O projeto de CBDC do Brasil, que se chama DREX, é um caso particularmente interessante por que irá permitir não só a digitalização da moeda soberana (o Real), como também ativos da economia, como ações de empresas, créditos de carbono, imóveis, carros, etc... O site CBDC Tracker da Atlantic Council é uma excelente fonte para ver o status de projetos ao redor do mundo.

A crescente adoção dessas tecnologias promete revolucionar a maneira como fazemos negócios, investimos e consumimos, criando um futuro mais transparente, eficiente e conectado.

Fintechs x cibercrimes: o limiar entre exploração cibernética e evolução digital

Autora: Vanessa Bandeira
Consultora de Cibersegurança, pós-graduação em Cibercrimes

Não é difícil perceber que a tecnologia vem avançando e permeando as rotinas sociais. Esse cenário fica ainda mais nítido ao analisar os hábitos financeiros, os quais anteriormente caracterizavam-se pela utilização de cartões de crédito físicos. Ao voltar-se para o panorama atual, pode-se constatar a evolução com o advento das modalidades de pagamentos digitais, sendo o Near Field Communication(NFC) [1] um significativo vetor deste avanço.

As empresas de tecnologias financeiras (fintechs) foram as grandes contribuintes do advento do mercado financeiro digital, impulsionando a inclusão financeira de consumidores e empresas no mercado virtual [2]. Tornando os serviços que outrora eram

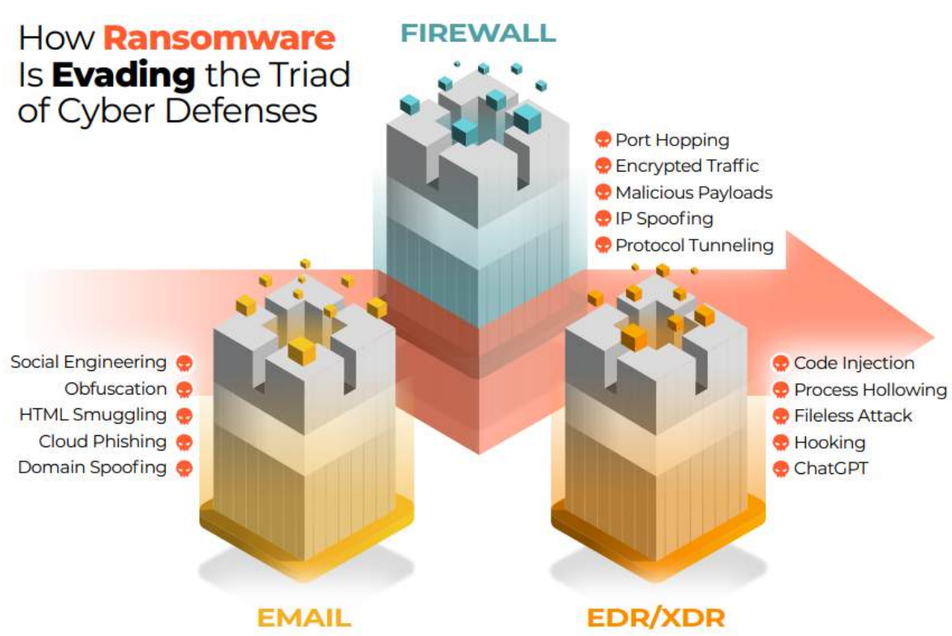


Fig 1: Técnicas de evasão da tríade da defesa cibernética [3]

executados de modo manual e burocrático, em atividades simples e desburocratizadas.

Todavia, a virtualização dos processos bancários por meio das fintechs trouxe consigo ameaças que até então estavam associadas a abordagens físicas, e que agora estão dispostas também em riscos voltados ao cibercrime financeiro.

A exploração de vulnerabilidades do ambiente pode ser realizada de diversas maneiras pelos hackers. Como pode ser observado na Figura 1, a qual evidencia as técnicas de evasão aplicadas a cada pilar da tríade da defesa cibernética.

Dentre as técnicas apresentadas, podemos destacar a engenharia social como uma das mais utilizadas, pois explora a vulnerabilidade humana. Esse cenário pode ser observado por meio de incidentes de segurança, como por exemplo o sofrido pela Evolve Bank and Trust, sediada em Arkansas, EUA. O ataque cibernético foi operado pelo grupo de ransomware LockBit [4], que utilizou como acesso inicial a técnica de phishing [5]. Por meio dela os atacantes tem como objetivo enganar usuários para que cliquem em links maliciosos ou abram arquivos infectados. Em adição ao phishing, os cibercriminosos utilizaram ransomware de criptografia de arquivos para executar o roubo dos dados da Evolve, bem como a extorsão financeira.

Além da camada de acesso inicial, o cenário frequentemente impactante ao setor de serviços financeiros, sob a ótica da cibersegurança, são os ataques de Distributed Denial of Service(DDoS)[6]. De acordo com o relatório elaborado pela Akamai [7], o setor de serviços financeiros, pelo segundo ano consecutivo, lidera consideravelmente a onda de ataques quando comparados a outros ramos da sociedade, como pode ser analisado na Figura 2.

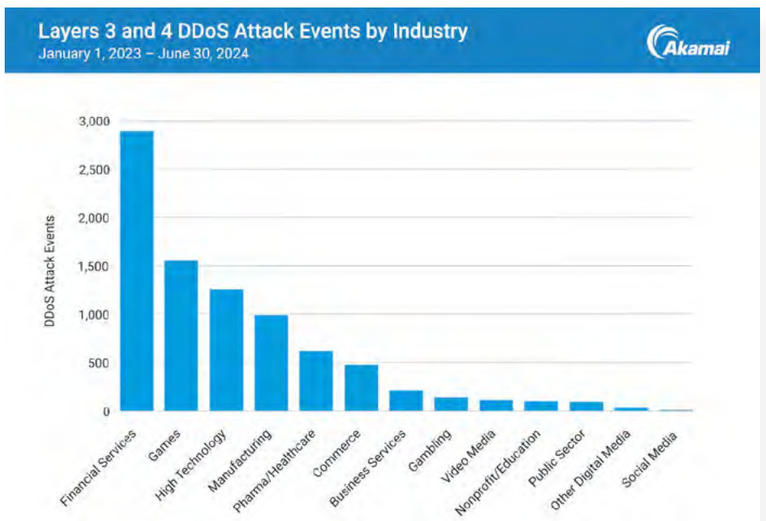


Fig 2: Figura 2 - DDoS em ramos da sociedade[7]

Esse panorama deixa evidente que, ao compasso do crescimento digital nos serviços financeiros, crescem as vulnerabilidades encontradas nas aplicações que são precursoras das potenciais explorações adversariais.

Considerando esses cenários de ameaças, se faz essencial que os bancos e as fintechs adotem tecnologias e estratégias de detecção e proteção contra ameaças. Um dos principais pontos de adoção de segurança associado às fintechs é a utilização da criptografia para a proteção dos dados trafegados durante as transações executadas pelos serviços financeiros, bem como a inclusão de uma ferramenta de segurança que protege aplicações web de ataques maliciosos, funcionando como uma barreira que filtra o tráfego entre o site e a internet.

No entanto, é importante deixar claro que não só a segurança em camadas deve ser o ponto essencial do setor de serviços financeiros, mas também devem ser feitos treinamentos voltados à educação em segurança cibernética. Dessa maneira, a camada de proteção se constrói sob o elo principal da sociedade, o ser humano.

Inovação Aberta: Colaboração entre grandes empresas, governos e startups

Autor: Edmilson Rodrigues do Nascimento Junior
Mestre em Ciências da Computação (UFPE)

Você já parou para se perguntar como as empresas e governos inovam?

Para Peter Drucker, o celebrado autor no ramo da Administração, Inovação é "a introdução de novas capacidades, processos ou métodos a fim de mudar o comportamento de agentes do mercado para criar e capturar mais valor para as firmas."

Contudo, a sabedoria da administração tradicional dizia que a inovação se dava em grandes empresas ou governos através de departamentos de Pesquisa e Desenvolvimento (P&D) que passavam por longos ciclos de criação de novos produtos. Empresas como a XEROX famosamente mantinham instalações como a XEROX PARC (Palo Alto Research Center), de onde surgiram inovações como a interface gráfica de computadores.

No entanto, esse modelo de inovação "fechada nos muros das empresas", apresentava suas fragilidades. Um exemplo de empresa que falhou em capitalizar sobre seus ciclos de inovação que ficou conhecido foi o da Kodak, gigante da era das máquinas fotográficas que desenvolveu em seus laboratórios a máquina digital, mas não soube reconhecer como aquela novidade iria impactar seu próprio negócio.

Em 2006, o Prof. Henry Chesbrough de Oxford lançou um livro que observava a ascensão de uma nova tendência: e se a inovação não se desse somente dentro dos muros de nossas organizações, mas pudesse ser feita de forma colaborativa com outros agentes da sociedade? A esse novo paradigma, deu-se o nome de "Open Innovation", ou Inovação Aberta.

De forma resumida, Inovação aberta é um paradigma que assume que as organizações, sejam empresas ou governos, podem e devem usar ideias externas, bem como ideias internas, e caminhos internos e externos para o mercado, na busca pelo avanço tecnológico. Sendo assim, a inovação aberta é a utilização de fluxos deliberados de conhecimento para acelerar a inovação interna e expandir os mercados para o uso externo da inovação. Ela pode se dar na forma de aquisição de empresas menores, ou organização de hackathons (concursos de idéias ou protótipos criados em um curto espaço de tempo), ou na execução de projetos de pesquisa em associação com outras empresas, universidades ou equipes de indivíduos, ou ainda na publicação de desafios organizacionais e na atração de equipes de inovadores para trabalhar nos desafios.

Um exemplo de empresa que vem adotando isso com maestria é a AMBEV, multinacional da produção de bebidas. Eles têm diversas iniciativas de inovação aberta, mas uma que se destaca é o programa "Além", que publica desafios anuais que a companhia gostaria de solucionar através da colaboração com startups. Outro exemplo, dessa vez no mundo das instituições financeiras, o Banco Bradesco, que mantém um ambiente físico de co-inovação chamado "Habitat" onde provê um escritório gratuito para startups e um ambiente de colaboração digital entre corporações e startups chamado "InovaBra".

É interessante observar que a inovação aberta também vem sendo adotada não só por empresas, mas também por governos ou organizações de interesse público. Por exemplo, o Banco Central do Brasil organiza os LIFT Labs (Laboratório de Inovação Financeira e Tecnológica), que articula empresas, universidades e startups para pesquisarem sobre e buscarem soluções para os principais desafios do sistema financeiro. Também, o Fórum Econômico Mundial criou uma plataforma chamada Uplink, que busca ser um articulador entre os desafios, financiadores e grupos de inovadores ao redor do mundo que possam ajudar a resolvê-los.

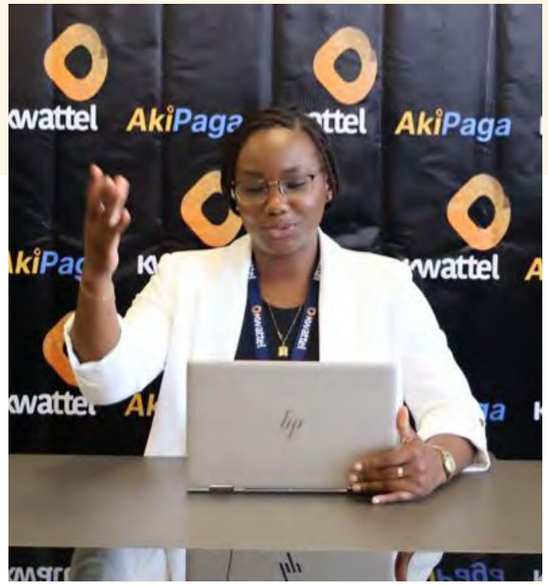
Portanto, seja em grandes empresas ou no governo, a inovação não deve acontecer somente dentro dos muros das organizações, mas pode ser conduzida de forma aberta e colaborativa com startups, universidades, pesquisadores e até através de consórcios entre concorrentes. Melhor ainda se feita de forma habilitada por plataformas digitais.

Mas é importante lembrar que a inovação aberta não é uma solução mágica para todos os desafios que as empresas enfrentam. A chave para o sucesso está na adoção de uma abordagem estratégica, com uma clara compreensão dos desafios e limitações, e na construção de processos e sistemas que possibilitem a criação de valor a partir da colaboração.

Remessas

Entrevista - Remessas em Angola já são uma realidade

Entrevistador: Adérito Veloso
Entrevistada: Plácida Savo



Há um ano, a Kwattel – Serviços de Pagamento, S.A. lançava o **1º Serviço de Remessas para o Exterior via Mobile Money em Angola** na sua plataforma de pagamentos móveis AkiPaga. Editamos na íntegra as perguntas que foram feitas na altura pelo jornalista Adérito Veloso, do Jornal de Angola.

Adérito Veloso – O que é o Serviço de Remessas AkiPaga?

Plácida Savo – É um serviço de transferências internacionais, disponibilizado através do canal USSD, com o qual o cliente poderá enviar e receber dinheiro directamente da sua carteira AkiPaga, para o exterior do país e vice-versa. O envio poderá ser para outras carteiras digitais e até mesmo para bancos, mas o recebimento será sempre na sua carteira AkiPaga

Adérito Veloso — Atendendo as diversas soluções já existentes no país para envio de dinheiro ao exterior, qual será o diferencial desta solução no mercado?

Plácida Savo – A nossa solução destaca-se pelas transacções ocorrerem de forma instantânea; ou seja, as transacções acontecem na hora sem a necessidade de períodos de espera para compensações. Em adição a esta valência, os nossos clientes não precisam ter conta bancária, poderão efectuar as suas transacções tanto num smartphone como num telefone analógico (vulgo Bombinha). Não precisam de saldo de dados ou de voz para acesso ao serviço, e podem efectuar as suas transacções em qualquer parte do país e a qualquer hora. E obviamente, com um custo inferior ao praticado no mercado, sendo que a Kwattel por ser uma Fintech, não possui a mesma estrutura de custos das instituições financeiras tradicionais.

Adérito Veloso – Quais serão os requisitos de acesso ao serviço?

Plácida Savo – Para ter acesso ao serviço de remessas da kwattel, o cliente deverá estar registado na plataforma de pagamentos AkiPaga (*447#), e tornar-se num cliente premium ligando para o nosso apoio ao cliente 923 166 680. Terão prioridade de habilitação ao menu para as remessas, os nossos clientes que já possuem um histórico de utilização activa na plataforma.

Adérito Veloso – Sendo que os clientes não precisam de uma conta bancária, como estes últimos carregarão as suas contas para a utilização do serviço?

Plácida Savo – O meio de carregamento e levantamento de dinheiro nas carteiras AkiPaga não foram alterados; ou seja, continua sendo a partir dos nossos Agentes AkiPaga espalhados em todo país. E para alternativas de carregamento, temos a possibilidade de transferência bancária nas contas oficiais da Kwattel, conforme publicação nas nossas redes sociais @AkiPaga Angola (Instagram, Facebook e LinkIdin), ou ainda no nosso website: www.kwattel.com. E em caso de dificuldade, o utente poderá entrar em contacto com a nossa rede de apoio ao cliente 923 166 680 das 7h:30 às 18h:30 nos dias úteis, para o devido auxílio.

Adérito Veloso – Quais são os países nos quais já é possível o envio das remessas?

Plácida Savo – Neste momento já é possível fazer o envio para mais de 31 países no mundo, dentre eles a China, Brasil, Portugal, Turquia, Emirados Árabes Unidos, Congos, Senegal, Ghana, África do Sul, Guiné e Moçambique.
A lista completa dos países está divulgada no nosso website, bem como os respectivos códigos dos países e dos bancos, para preenchimento aquando do envio das remessas.

Adérito Veloso – Relativamente aos limites de valores a serem enviados?

Plácida Savo –

> *A grande premissa desta solução financeira e tecnológica é a de oferecer a todos os cidadãos a possibilidade de apoiar as suas famílias no exterior do país, bem como estes no exterior, apoiarem os seus familiares em Angola.*

Portanto, serão valores cuja maior parte do uso se destina a ajuda de custos para com a saúde, educação e peças sobressalentes; ou seja, despesas essenciais. A princípio será possível enviar e receber até 250 Euros por mês. O nosso objectivo é crescermos o valor de remessas logo que ultrapassarmos os constrangimentos de acesso às divisas. Desta forma, a Kwattel traz uma nova forma de investimento, e convida os investidores que têm o seu dinheiro parado, pessoas com depósitos em moeda estrangeira, a investirem no Fundo de Investimento da Kwattel (FIK), e desta forma rentabilizarem o seu capital.

Adérito Veloso – Em termos de segurança, quais são as garantias que a Kwattel oferece aos seus clientes?

Plácida Savo – O envio e recebimento de remessas constitui mais um dos muitos serviços agregados e que continuarão sendo agregados a plataforma de pagamentos AkiPaga. Esta por sua vez uma plataforma segura, actuando no mercado desde 2021 e até ao momento não registamos nenhum incidente. A Kwattel utiliza tecnologia de segurança de última geração, encriptação ponto à ponto que mantém a sua conta e operações financeiras totalmente seguras, e confidenciais, bem como o reconhecimento digital em cada transacção por efectuar (PIN). A Kwattel também é autónoma relativamente ao processamento e armazenamento dos dados das transacções, possuindo 2 Data Centers para o efeito. Mas obviamente, apelamos sempre aos nossos clientes o cuidado redobrado com os seus dados pessoais, e aquando da utilização dos mesmos, garantirem sempre que ninguém consegue ver ou ter acesso indevido a tais informações.

Adérito Veloso – Em termos económicos, quais serão as principais contribuições do Serviço de Remessas da Kwattel?

Plácida Savo – É um serviço tecnológico e inovador em Angola, que surge para contribuir com a inclusão financeira. O intuito é contribuir para a queda do nível de venda de divisas no mercado informal (mercado de câmbio das ruas), bem como diminuir os processos ilícitos de venda de divisas, que infelizmente vem crescendo e com taxas destruidoras dos parcos recursos das famílias e de pequenos empresários.
Com o serviço de Remessas a Kwattel pretende facilitar as transferências entre o público digital e os que não estão familiarizados com a modernidade, erradicando os problemas de acesso a serviços financeiros, com custos baixos e promover um ambiente institucional mais eficiente em termos de regulamentação, concorrência e inovação.
O sistema de Pagamentos móveis, é uma das principais soluções a nível de África para a formalização da economia, apoiando as políticas governamentais nas estratégias de reforma económica. Com os seus custos baixos, promove a poupança, e consequentemente a geração de riqueza. A partir das PSP's, o dinheiro que circula no mercado informal, é reconvertido para o sistema financeiro real, em forma de pagamentos de

impostos, e outras obrigações pagas por estas ao Governo. Sem esquecer que o Mobile Money reduz significativamente o custo de emissão de moeda, e aumenta os níveis de segurança dos utentes na utilização dos seus recursos financeiros.

Adérito Veloso – Draª Plácida Savo, estamos na recta final da nossa entrevista, gostaria de acrescentar algum ponto, ou tecer algumas considerações finais?

Plácida Savo – Dizer que estamos muito orgulhosos em ser a primeira empresa angolana a oferecer esse serviço aos nossos cidadãos. Estamos a responder uma necessidade dos angolanos em geral, e dos imigrantes legais no nosso país.
Quero realçar que temos recebido muitos pedidos de angolanos no exterior, que tencionam ajudar as suas famílias aqui no país, e esse processo também já é possível na AkiPaga. Não podemos esquecer que as remessas contribuem significativamente na obtenção de divisas.

> *A Kwattel continuará inovando no âmbito da sua política de inclusão financeira e digital, alinhada a Estratégia Nacional de Inclusão Financeira, já que temos mais do que a metade da população fora do sistema financeiro real.*

Com os nossos serviços visamos contribuir para uma economia mais saudável, diminuindo os dólares falsos e operações fraudulentas ou sem respaldo legal no sistema financeiro real.

A problemática das remessas no continente africano

Autor: Sebastian Rafael
Analista de Mercados

Um dos ganhos em África tem sido o uso, ainda por generalizar, das Carteiras digitais. Estas, vulgarmente conhecidas como "Wallet", são igualmente facilitadoras da inclusão financeira e de conforto de serviços digitais num clique, e com rapidez e eficiência superiores ao burocratizante serviço bancário tradicional que tem perdido agências junto das comunidades periféricas.

Em Angola, a Wallet AkiPaga da KWATTEL, numa visão de sedimentação das suas valências digitais, lançou, em 2024, o serviço de Remessas para mais de 38 países. Naturalmente, em mercados maduros, onde o sistema de pagamentos é desenvolvido no interesse dos cidadãos, o resultado dessa funcionalidade reforçaria o crescimento e a solidez da utilidade das Fintechs de Remessas, leiam o caso de sucessos da Western Union, MoneyGram, Revolut, Zepz e Prex, só para citar as cinco grandes empresas de Remessas de várias regiões do mundo.

Depois do surgimento da primeira Fintech angolana de Remessas, seria importante que, no interesse de contramedidas oportunas contra a venda ilícita de divisas espalhadas um pouco por todas as grandes urbes do país, colocassem em prática uma estratégia que permitisse que wallets como AkiPaga satisfazesse as suas necessidades de aquisição de divisas, uma ação que diminuiria o impacto negativo e corrosivo dos canais ilícitos que funcionam à luz do dia.

O objetivo das Remessas, mesmo quando se compra no paralelo, tem um forte impulso das necessidades de as famílias adquirirem divisas para pagarem as Propinas, as contas de Saúde e necessidades de compra de Peças sobressalentes para os seus meios rolantes, dizem os estudos.

O que pretendo realçar em termos de positividade é a existência de uma ferramenta denominada AkiPaga que deve estar no centro das contramedidas oficiais, através de acordos e instrutivos que facilitem as compras de moedas. Não se pode esvaziar uma Fintech que tenha esse potencial, e é urgente que se crie o bom ambiente de cooperação baseado nos valores de normalidade do sistema de Remessas.

Deve-se ter em conta que devido a auto regra da AkiPaga ao estabelecer os limites dos montantes, fixados nos mil euros, certamente o público alvo serão os portadores de telefones, vulgo bombinhas, que têm em mãos e no teclado do telefone o poder instantâneo de apoiarem ou receberem de seus filhos emigrantes as ajudas básicas. A operacionalidade do "inbound", certamente irá permitir que os emigrantes enviem igualmente pequenos valores que fazem toda difereça socialmente.

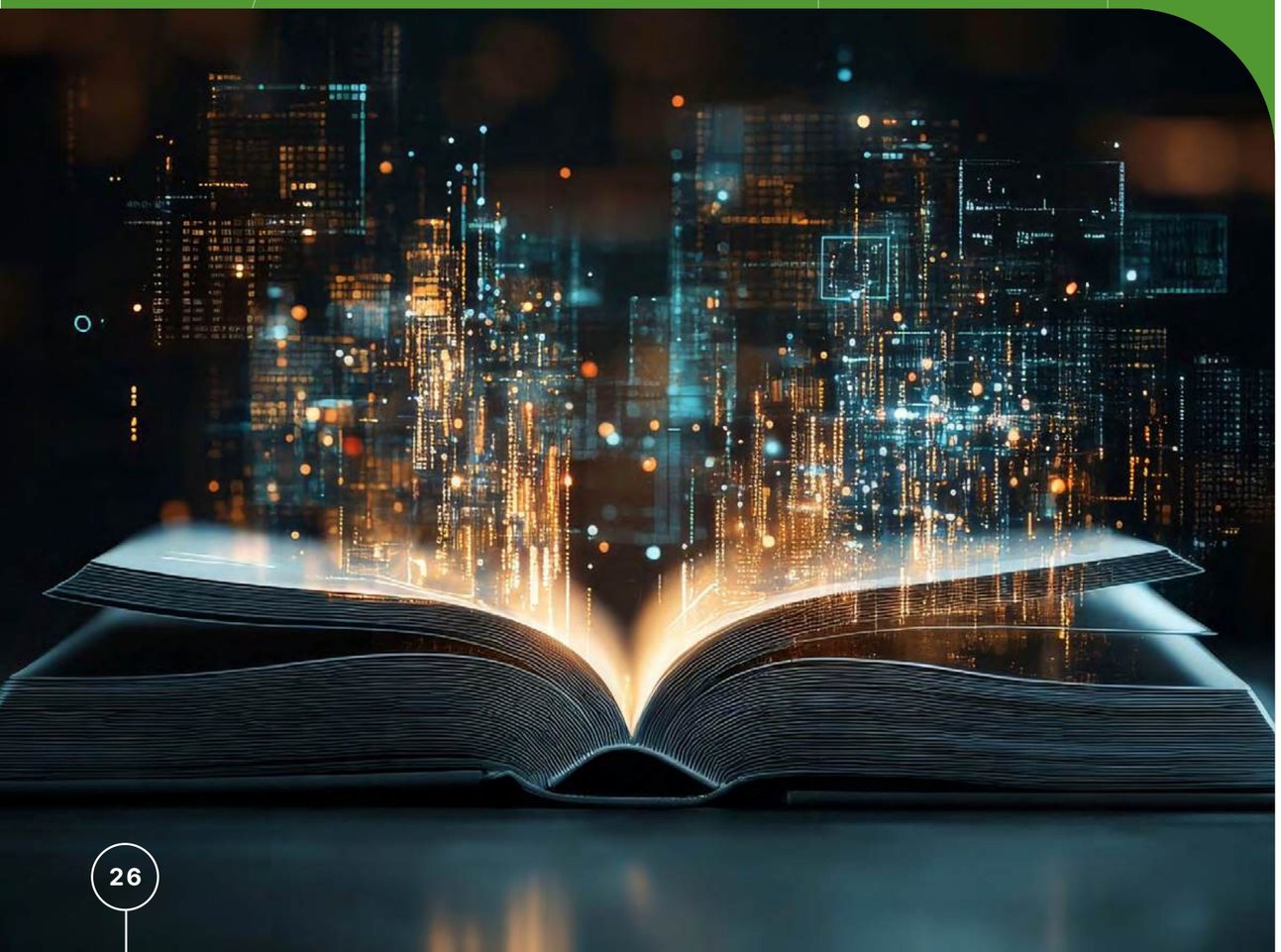
Vejamos o impacto social: Cinquenta euros a receber de fora são equivalentes a 53 mil kz, valores que aumentarão os meios de sobrevivência das famílias de baixa renda ou da classe média baixa que mais sofrem com a atual situação de dificuldades sociais por falta de fontes regulares de rendimentos e uma inflação situada nos dois dígitos.

Interessa realçar que nem os departamentos governamentais que acompanham o sistema de pagamentos e muito menos os Bancos Centrais dos países africanos podem perder esse jogo de normalidade, naturalmente com vantagem funcional das Fintechs autorizadas, pois não pode o forte sistema paralelo de venda de divisas ser quem mais satisfaz em tempo útil os cidadãos que procuram por um serviço eficiente à altura das suas demandas.

Textos críticos e Relatórios têm registrado que o negócio atinge as impressionantes somas de vendas de divisas. Em Africa a venda de divisas nas ruas e mercados populares tem estado sempre em alta. O maior risco é a sua normalidade e domínio, infelizmente hoje em triângulos que estabelecem os links de operabilidade entre moedas locais e o moedas fortes.

Assim, a existência das valências da KWATTEL, como primeira operadora digital de Remessas de Angola deve ser incentivadora de respostas institucionais como contramedidas que melhorem a economia, um desiderato que consiga iliminar o cancro referido e que tem provocado ferozes anormalidades de alto risco do sistema.

Dicionário de Cibersegurança



Breve Dicionário de Cibersegurança

Autora: Conceição Inglês
Diretora Administrativa da Iguana Comunicações

Num mundo cada vez mais digital, a cibersegurança deixou de ser um tema técnico reservado a especialistas para se tornar uma preocupação comum a empresas, governos e cidadãos. Este breve dicionário reúne conceitos essenciais para entender melhor esta área crítica, que visa proteger os nossos dados e sistemas de informação contra ameaças e ataques cibernéticos.

O que é a Cibersegurança?

É a prática de proteger redes, sistemas e infraestruturas digitais contra ataques maliciosos. Num cenário onde os ataques cibernéticos ocorrem a cada 14 segundos, a cibersegurança surge como a última linha de defesa contra o caos digital, protegendo empresas e indivíduos contra o roubo e a exposição de dados.

Segurança da Informação

Diferente da cibersegurança, a segurança da informação tem uma abordagem mais abrangente, focada na protecção de dados em qualquer ambiente — seja digital ou físico. A cibersegurança, por sua vez, é um subconjunto que actua especificamente nos meios digitais.

Malware

Termo genérico para software malicioso, como vírus, spyware e ransomware. Normalmente, entra nos sistemas através de falhas, e-mails suspeitos ou apps perigosas, podendo roubar dados, danificar sistemas ou bloquear o acesso a informações vitais.

Phishing

Técnica que consiste em enviar e-mails fraudulentos que imitam fontes confiáveis para induzir as vítimas a fornecer dados sensíveis, como logins e informações bancárias.

Engenharia Social

Manipulação psicológica de indivíduos para obtenção de informações confidenciais. Pode ocorrer por e-mail, telefone ou redes sociais. Um exemplo avançado é a clonagem de voz para enganar amigos e familiares.

Ataque Man-in-the-Middle (MitM)

Quando um hacker intercepta a comunicação entre duas partes — como num Wi-Fi público — para aceder a informações sem ser detectado.

Ataque de Dia Zero

Ocorre quando cibercriminosos exploram uma vulnerabilidade recém-divulgada antes que a empresa afectada consiga lançar uma actualização de segurança (patch).

Segurança de Aplicações

Refere-se à implementação de defesas dentro de software e serviços para prevenir acessos não autorizados e alterações maliciosas.

Segurança de Dados

Foca-se na protecção da informação tanto em repouso como em trânsito, com sistemas de armazenamento robustos e encriptados.

Segurança de Rede

Conjunto de medidas para prevenir o uso indevido, interrupções e acessos não autorizados à rede interna de uma organização.

Segurança em Dispositivos Móveis

Abrange medidas de protecção para smartphones, tablets e laptops, que são frequentemente usados para aceder a dados empresariais sensíveis.

Segurança na Nuvem

Garante a protecção de sistemas e aplicações baseados em cloud computing contra ameaças virtuais, frequentemente através de ferramentas como firewalls e inteligência artificial.

Pen Test (Teste de Intrusão)

Simulação de ataques cibernéticos para avaliar a eficácia das defesas de uma organização. Pode envolver testes à infraestrutura, aplicações web ou simulações de ataques reais (red teaming).

Testes de Segurança Contínuos

Diferente do Pen Test tradicional, são realizados regularmente para acompanhar aplicações em constante evolução e descobrir vulnerabilidades a tempo.

Vulnerability Assessment (Avaliação de Vulnerabilidades)

Processo de identificação e priorização de falhas de segurança em sistemas, redes e aplicações, utilizando scanners especializados.

SOC – Security Operations Center

Centro de Operações de Segurança que monitoriza e responde a incidentes 24/7, actuando rapidamente em caso de ataques cibernético

WAF – Web Application Firewall

Firewall que protege aplicações web e APIs contra ataques, recorrendo a tecnologias como machine learning para detectar padrões de ameaça.

DevSecOps

Integração da segurança no processo de desenvolvimento de software, com revisão de código desde a fase inicial para reduzir vulnerabilidades antes mesmo do lançamento.

Endpoint Security

Segurança aplicada a dispositivos finais (computadores, telemóveis, etc.), especialmente quando estão fora da rede corporativa, garantindo acesso seguro a sistemas e dados.

SIEM – Security Information and Event Management

Solução que centraliza a gestão de eventos e informações de segurança, permitindo identificar comportamentos anómalos e prevenir violações.

Referências Bibliográficas

Necessidade de investimento em Cibersegurança em Angola

[1] Angola é um dos cinco países mais atacados por hackers – DW – 18/10/2021 --- dw.com. https://www.dw.com/pt-002/angola-governo-admite-que-%C3%A9-preciso-um-centro-para-combater-o-cibercrime-no-pa%C3%ADs/a-59536562, [Accessed 30-09-2024]

[2] DDoS Attack Trends for 2022 Q1 - Cloudflare Radar - 12/04/2022 https://radar.cloudflare.com/reports/ddos-2022-q1, [Accessed 30-09-2024]

[3] Security & Attacks Angola - Cloudflare Radar - 30/09/2024 https://radar.cloudflare.com/security-and-attacks/ao?dateRange=28d, [Accessed 30-09-2024]

[4] Ataque Cibernético à Sonangol --- makaangola.org. https://www.makaangola.org/2019/08/ataque-cibernetico-a-sonangol/, [Accessed 30-09-2024]

[5] Ataque Cibernético no Banco Nacional de Angola --- makaangola.org. https://www.makaangola.org/2024/01/ataque-cibernetico-no-banco-nacional-de-angola/, [Accessed 30-09-2024]

[6] Agência Lusa. Transportadora aérea angolana TAAG alvo de ataque cibernético --- observador.pt. https://observador.pt/2024/09/16/transportadora-aerea-angolana-taag-alvo-de-ataque-cibernetico/, [Accessed 30-09-2024]

[7] grxnet.com. Ministério das Telecomunicações, Tecnologias de Informação e Comunicação Social - Projectos --- minttics.gov.ao. https://minttics.gov.ao/ao/projectos/, [Accessed 30-09-2024]

Tecnologia Blockchain e Tokenização de ativos

Central Bank digital currency tracker. Disponível em: <https://www.atlanticcouncil.org/cbdctracker/>. Acesso em: 21 set. 2024.

Global payments & financial solutions for businesses. Disponível em: <https://ripple.com/>. Acesso em: 22 set. 2024.

Mento Labs. Disponível em: <https://www.mentolabs.xyz/>. Acesso em: 22 set. 2024.
NAKAMOTO, Satoshi. Bitcoin: Um Sistema de Dinheiro Eletrônico Peer-to-Peer. 2008. Acesso em: 20 set. 2024.

NOE, Rain. *A medieval British anti-counterfeiting system: Split tally sticks.* Disponível em: <https://www.core77.com/posts/67600/A-Medieval-British-Anti-Counterfeiting-System-Split-Tally-Sticks>. Acesso em: 20 set. 2024.

Preços, Gráficos e Capitalização de Mercado das Criptomoedas. Disponível em: <https://coinmarketcap.com/pt-br/>. Acesso em: 20 set. 2024.

SUCH-GUTIÉRREZ, Marcos. A invenção da escrita cuneiforme pelos sumérios. National Geographic, 23 jan. 2023. Disponível em: <https://www.nationalgeographic.pt/historia/a-invencao-da-escrita-cuneiforme-pelos-sumerios_3457>. Acesso em: 20 set. 2024.

Fintechs x cibercrimes: o limiar entre exploração cibernética e evolução digital

[1] KONAIAGARI, A. NFC payments: Working, benefits, concerns, and future. Disponível em: <https://www.pluralonline.com/nfc-payments-working-benefits-concerns-and-future/>. Acesso em: 19 oct. 2024.

[2] BLAKSTAD, S.; ALLEN, R. FinTech revolution. Cham: Springer International Publishing, 2018.

[3] BROWN, J. Lumu's ransomware infographic: The 2023 ransomware flashcard. Lumu Technologies, 17 Apr. 2023. Disponível em: <https://lumu.io/blog/2023-ransomware-infographic/>. Acesso em: 20 oct. 2024

[4] KOVACS, E. Evolve Bank Shares Data Breach Details as Fintech Firms Report Being Hit. Disponível em: <https://www.securityweek.com/evolve-bank-shares-data-breach-details-as-fintech-firms-report-being-hit/>. Acesso em: 19 oct. 2024.

[5] THE MITRE CORPORATION. MITRE ATT&CK AND ATT&CK. Phishing. Disponível em: <https://attack.mitre.org/techniques/T1566/>. Acesso em: 19 oct. 2024.

[6] THE MITRE CORPORATION. MITRE ATT&CK AND ATT&CK. Network Denial of Service. Disponível em: <https://attack.mitre.org/techniques/T1498/>. Acesso em: 19 oct. 2024.

[7] MAYNE, M. Beware the Rising Tide: Financial Services Is Awash in Attacks. Disponível em: <https://www.akamai.com/blog/security-research/financial-services-is-awash-in-attacks>. Acesso em: 19 oct. 2024.

Inovação Aberta: Colaboração entre grandes empresas, governos e startups

Além. Programa de Inovação Aberta da Ambec. Disponível em: <https://www.ambev.com.br/alem>. Acesso em: 21/9/2024.

Banco Central do Brasil. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/lift>. Acesso em: 21/9/2024.

CHESBROUGH, Henry. Open innovation: a new paradigm for creating and profiting from technology. Boston: Harvard Business School Press, 2003.

Inovabra. Banco Bradesco. Disponível em: <https://www.inovabra.com.br/html/pt/para-startups.shtm>. Acesso em: 21/9/2024a.

UpLink. World Economic Forum.Disponível em: <https://uplink.weforum.org/>. Acesso em: 21/9/2024.

iguana

CONTACTOS

Tlm: 921 997 205
Tlf: 939 291 946
E-mail: geral@iguanalda.com

MORADA

Rua Camilo Pessanha,
Nº28-B, Vila Alice - Rangel
Luanda, Angola

iguanalda.com