
SpeedNet
IT E TELECOMUNICAÇÕES
Security Strategy | Data Protection | Risk Management | Operations
Webinar | Transformação Digital e o papel da Segurança Cibernética
SPEEDNET- Direção de Segurança Cibernética
Setembro, 2020

SOBRE NÓS:

Somos uma empresa angolana licenciada pelo **INACOM (Instituto Nacional das Comunicações)** e registada no **INFOSI (Instituto Nacional de Fomento da Sociedade da Informação)** que atua no setor das Telecomunicações e Tecnologias de Informação (TI), como operador de Telecom, prestador de serviços, Integrador de Soluções de TI e Sistemas Informáticos (SI) com foco mas não limitado em:

Infra-estruturas:

✓ Infra-estrutura de Rede Interna do cliente (desde a rede estruturada à equipamentos activos);
✓ Infra-estrutura de Rede em Fibra-Óptica e Rádio Frequências;

Comunicações:

✓ VPN's L2/L3 / SD-WAN;
✓ Internet Dedicada / QoS (Partilhada);
✓ Plataformas de Segurança Unificadas (UTM);

Soluções de TI & Consultoria:

✓ Cyber Security;
✓ SOCaaS - Security Operating Center as a Service;
✓ Integração de Sistemas, Gestão e Manutenção de Sistemas IT.
✓ Soluções integradas de CCTV (com possibilidade de Public/Private Cloud) e Corporate TV (IPTV).

Somos uma empresa focada na entrega de soluções feitas à medida e abordamos todas as oportunidades como projectos que devem ser geridos de forma minuciosa, sempre focamos nos objectivos de negócio do cliente.

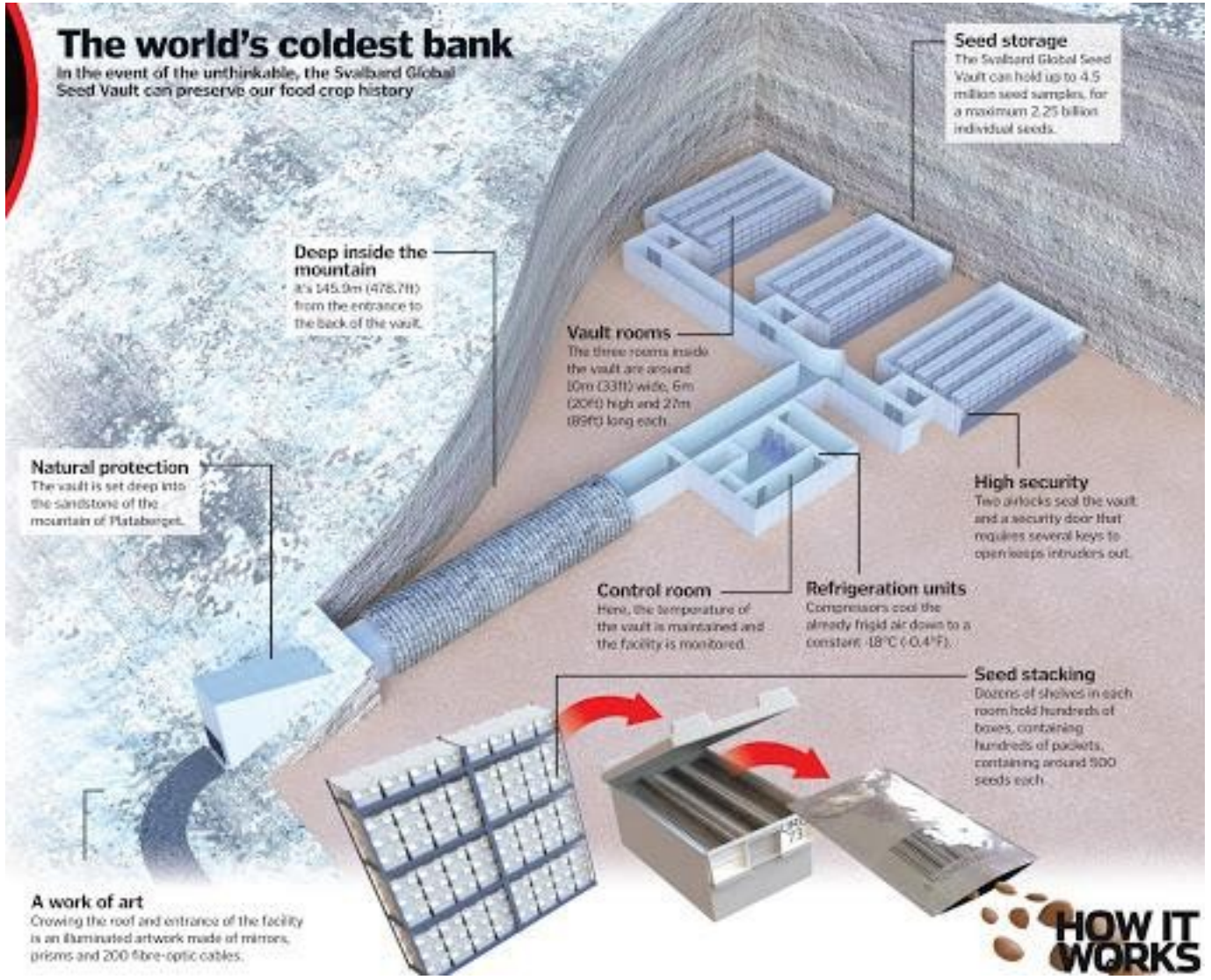
Para atender as necessidades e níveis de exigência dos clientes, dispomos de uma equipa de técnicos especialistas nas suas diferentes áreas de actuação, com anos de experiência e certificação necessária para dar cobro, com qualidade aos projectos adjudicados.

Microsoft recupera data center que estava embaixo d'água há 2 anos

Equipamento ficou submerso na costa de Orkney, na Escócia, para testar sua eficiência energética nas profundezas do oceano; dos 855 servidores que funcionavam, apenas oito apresentaram defeitos.

15/09/2020

A pensar nas gerações futuras, o GitHub guardou todo o seu software de código aberto num “Cofre do Apocalipse” (Svalbard)



No último ano não houve melhoria na identificação e prevenção de riscos cibernéticos, um grande ponto cego que pode custar US $ 3 Mil Milhões

2 dos 5 maiores riscos globais estão ligados à cibersegurança

•De acordo com o Global Risks Report 2019 do World Economic Forum, na perspectiva de 10 anos da pesquisa, os riscos cibernéticos sustentaram significativamente em relação ao registrado em 2018.

•A grande maioria dos entrevistados espera pelo aumento de ataques cibernéticos, levando ao roubo de dinheiro e de dados (82%) e à interrupção das operações (80%).

Types of Risks: ENVIRONMENTAL GEOPOLITICAL SOCIETAL TECHNOLOGICAL ECONOMIC

Top 5 Global Risks in Terms of **Impact**

1. Weapons of mass destruction
2. Failure of climate-change mitigation and adaptation
3. Extreme weather events
4. Water crises
5. Natural disasters

Top 5 Global Risks in Terms of **Likelihood**

1. Extreme weather events
2. Failure of climate-change mitigation and adaptation
3. Natural disasters
4. Data fraud or theft
5. Cyber-attacks

SOURCE: World Economic Forum – Global Risks Report 2019

O que é o Risco Cibernético?

Risco à Reputação

- Perda de confiança (interna e externa)
- Dano à marca/Perda de valor intangível
- Perdas em custo e tempo para reparar
- Melhor a prevenção do que a remediação

Tecnologia e Risco Operacional

- Falha de infraestrutura, processos ou sistemas
- Incapacidade de operar / administrar os negócios
- Requer um planejamento regular e supervisão
- Importância de controles eficazes e atuais

Fraude e Crimes Financeiros

- Perda de receita e lucro - alto custo
- Alta velocidade e alta frequência / incessantes
- Necessidade de acompanhar a agenda regulatória
- Requer soluções tanto para negócios como para tecnologia

Fontes Externas de Risco Cibernético

- Hacktivismo
- Hacker
- Ataques motivados
- Vazamento de dados
- Engenharia social

Origens Internas de Risco Cibernético

- Serviços Bancários digitais
- Pagamentos
- Negociação Eletrônica
- Terceiros
- Infraestrutura de Tecnologia

Banco chileno atingido por ransomware: 12 mil computadores congelados

Atacado por um ransomware que se supõe seja o Sodinokibi, o banco ontem só conseguiu abrir 24 das suas 417 agências.

08/09/2020

Em um pronunciamento, Sebastián Sichel, presidente da instituição, afirmou que os dados sobre os fundos dos 13 milhões de clientes não foram afetados e que as equipes de TI estão trabalhando para restaurar os sistemas internos. Ele não confirmou que o banco tenha recebido um ***pedido de resgate em criptomoedas***. No entanto, aproximadamente 12 mil computadores foram atingidos, disseSichel.

Fonte: https://www.cisoadvisor.com.br/banco-chileno-atingido-por-ransomware-12-mil-computadores-congelados/

Gestão do domínio “ao” será transferido para Angola

O domínio “ao”, cuja infraestrutura digital estava sediada em Portugal, era gerido, desde 1996, pelo Centro de Estudos da Faculdade de Engenharia da Universidade Agostinho Neto, via *UNINET*.

De acordo com o despacho nº 126, publicado em Diário da República de 21 de Agosto, a transferência da raiz principal do domínio “ao” tem como objectivo melhorar a eficiência da política de gestão da referida estrutura, de modo a reforçar a segurança e protecção da soberania digital do Estado angolano no ciberespaço.

Fonte: https://www.menosfios.com/gestao-do-dominio-ao-sera-transferido-para-angola/

RESILIÊNCIA CIBERNÉTICA

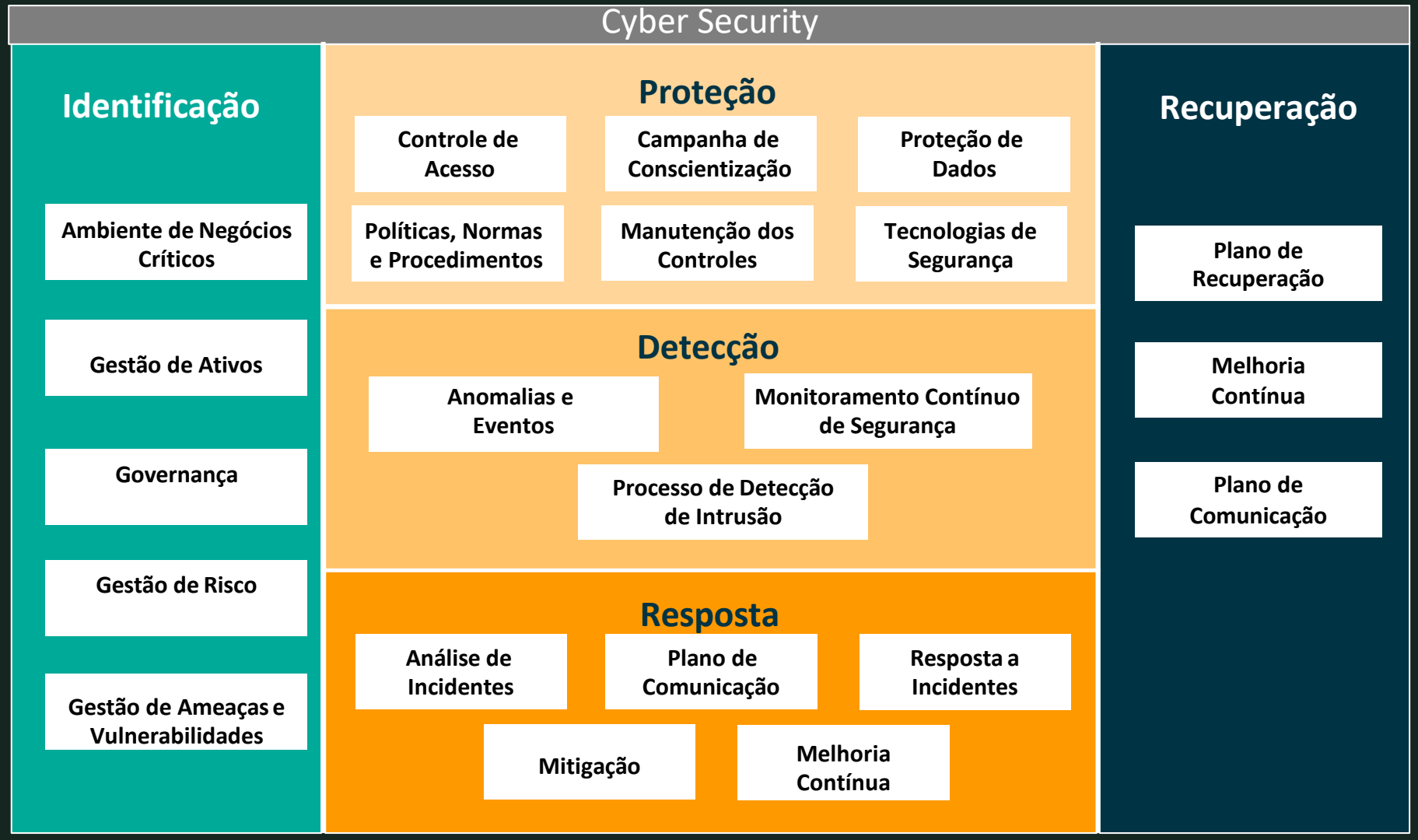
A capacidade de antecipar, absorver, adaptar e / ou rapidamente recuperar-se da interrupção causada por um ataque cibernético.

CYBER SECURITY

São as estratégias, políticas e normas para a redução de ameaças, vulnerabilidades, resposta a incidentes e resiliência cibernética.

ARQUITETURA DE REFERÊNCIA

RESILIÊNCIA CIBERNÉTICA



O que é o Risco Cibernético?

Risco à Reputação

- Perda de confiança (interna e externa)
- Dano à marca/Perda de valor intangível
- Perdas em custo e tempo para reparar
- Melhor a prevenção do que a remediação

Tecnologia e Risco Operacional

- Falha de infraestrutura, processos ou sistemas
- Incapacidade de operar / administrar os negócios
- Requer um planejamento regular e supervisão
- Importância de controles eficazes e atuais

Fraude e Crimes Financeiros

- Perda de receita e lucro - alto custo
- Alta velocidade e alta frequência / incessantes
- Necessidade de acompanhar a agenda regulatória
- Requer soluções tanto para negócios como para tecnologia

Fontes Externas de Risco Cibernético

- Hacktivismo
- Hacker
- Ataques motivados
- Vazamento de dados
- Engenharia social

Origens Internas de Risco Cibernético

- Serviços Bancários digitais
- Pagamentos
- Negociação Eletrônica
- Terceiros
- Infraestrutura de Tecnologia

Mil e 117 ataques cibernéticos contra empresas públicas, privadas e pessoas singulares foram registados no primeiro semestre deste ano em Angola

Os ataques à banca totalizaram os 6.9 por cento, enquanto os telemóveis suportaram 34,9 por cento, devido à inobservância de medidas de segurança por parte dos usuários.

A clonagem de cartões de crédito, transferências ilícitas via internet banking, venda simulada de produtos via Internet, espionagem e incitamento à violência como fatores que têm provocado prejuízos à economia.

Consta ainda da lista o acesso ilegítimo de programas, sabotagem e falsidade informáticas, inutilização do sistema informático, ameaças virtuais, fraude de computadores e programa espião.

28-08-2020 | Fonte: Jornal de Angola

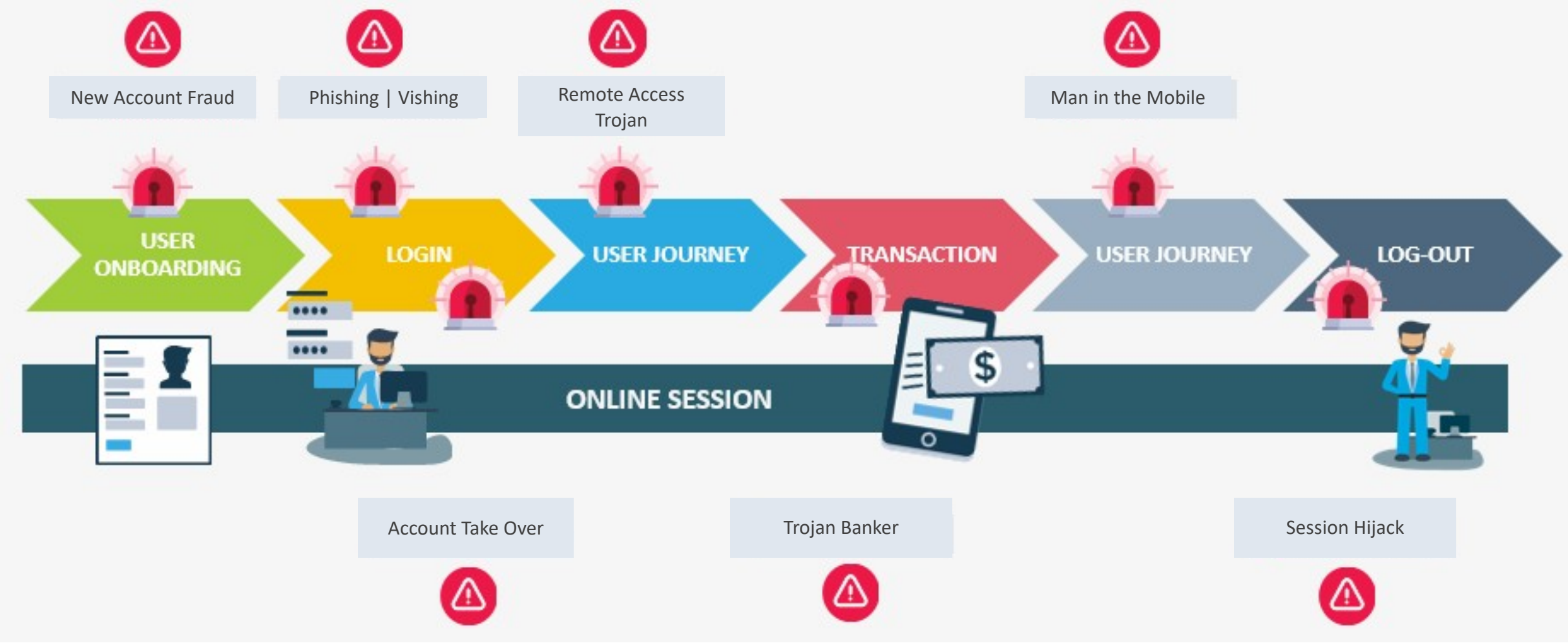
Combate à fraude on-line

Análise Comportamental + Análise do Dispositivo + Detecção de Malware

Biometria Comportamental

Ao analisar milhares de parâmetros em torno da pessoa, identificamos univocamente cada utilizador pelo seu comportamento durante toda a interação com o serviço online.

A jornada do cliente do banco



The Clear, Deep, and Dark Web

Clear Web

- Ferramentas de buscas, exemplo: Google.
- Media, Blogs, etc.

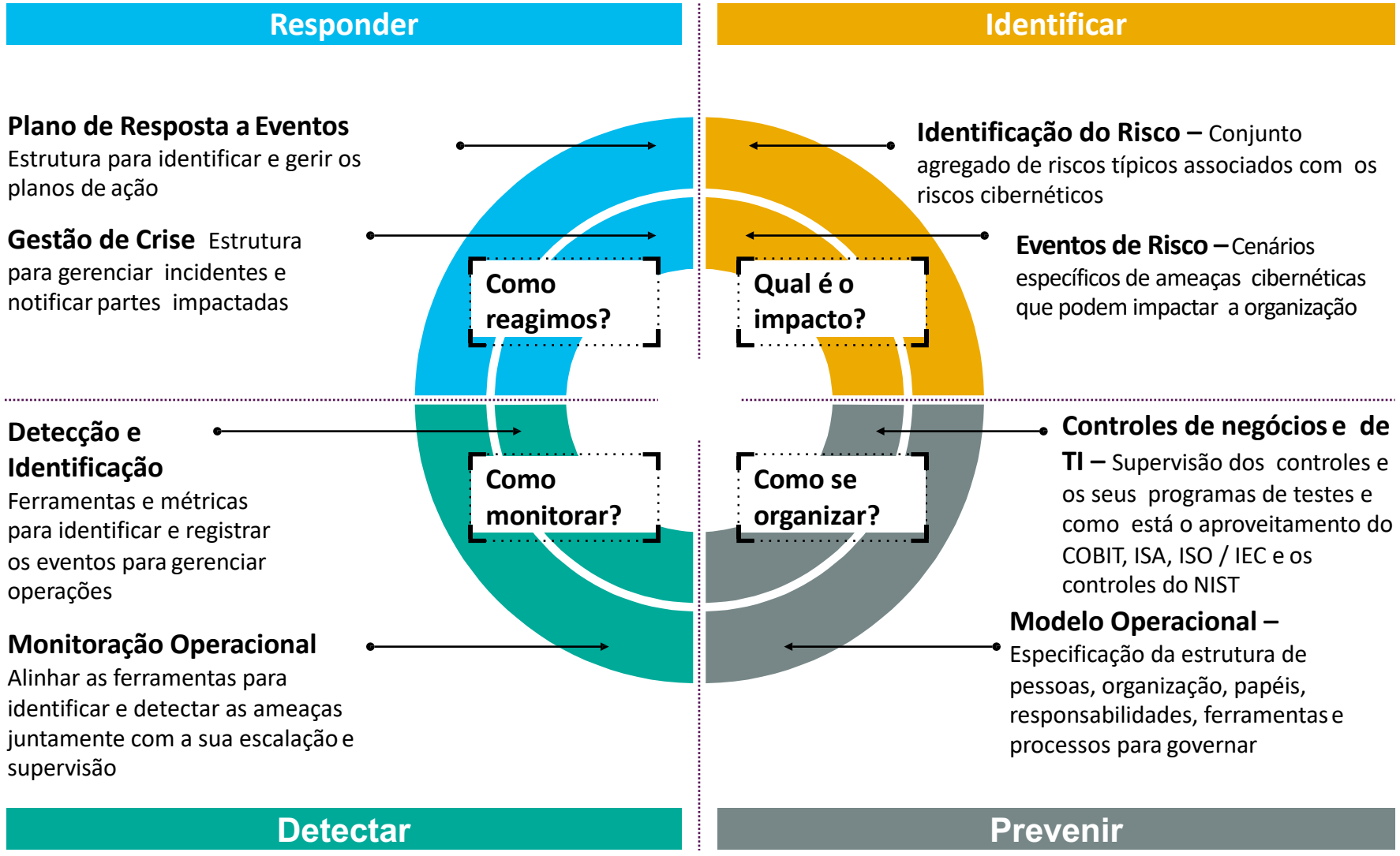
Deep Web

- Informações não indexadas.
- inclui partes privadas de diferentes portais, como o conteúdo da sua caixa de entrada de e-mail ou de um perfil privado do Facebook.

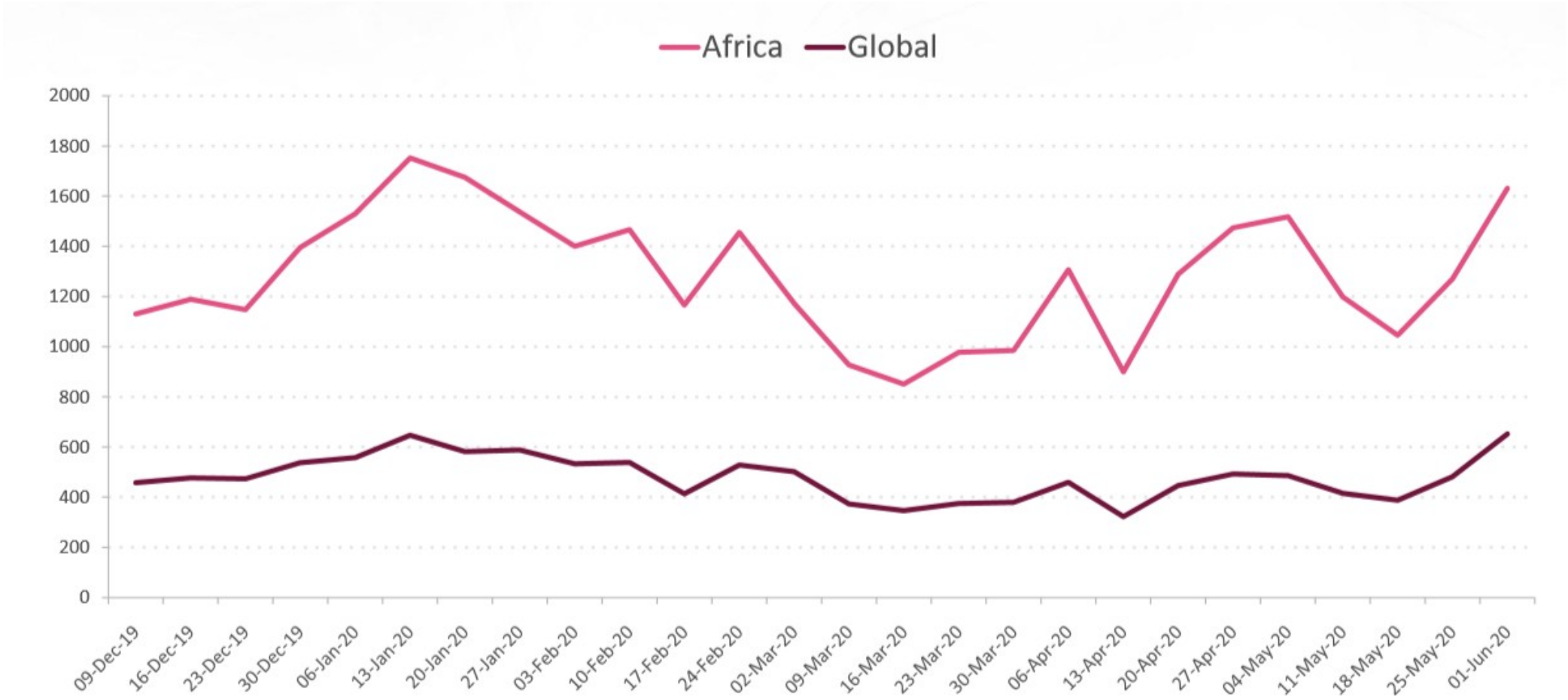
Dark Web

- Telegram, redes ponto a ponto (P2P), grupos fechados, apenas para convidados, foruns hacker.
- É usada para o compartilhamento de conteúdo ilegal, como venda de drogas, pedofilia e violência.

Como proteger todos os pontos de entrada e operações do banco



Continente Africano é o principal alvo dos ataques cibernéticos nos últimos 6 meses



Países mais atacados no continente Africano:
Angola é o 2° país que mais sofre ataques cibernéticos

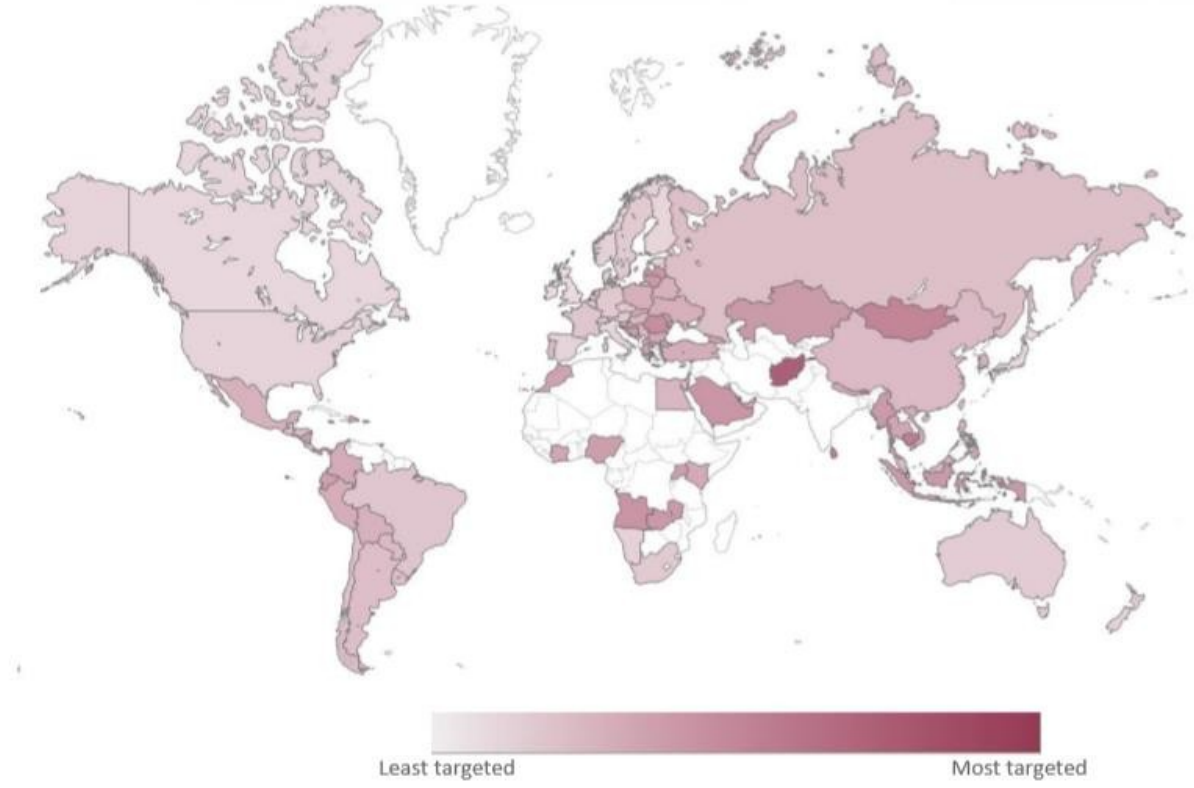
#1 Mauritius

#2 Angola

#3 Kenya

#4 Uganda

#5 Zambia



BNA quer implementar sistema de dinheiro digital no país

O Banco Nacional de Angola (BNA) lançou um pedido de informação com vista a selecionar a empresa que será responsável pelo Sistema de Transferências Móveis e Instantâneas ('mobile money') a implementar em Angola.

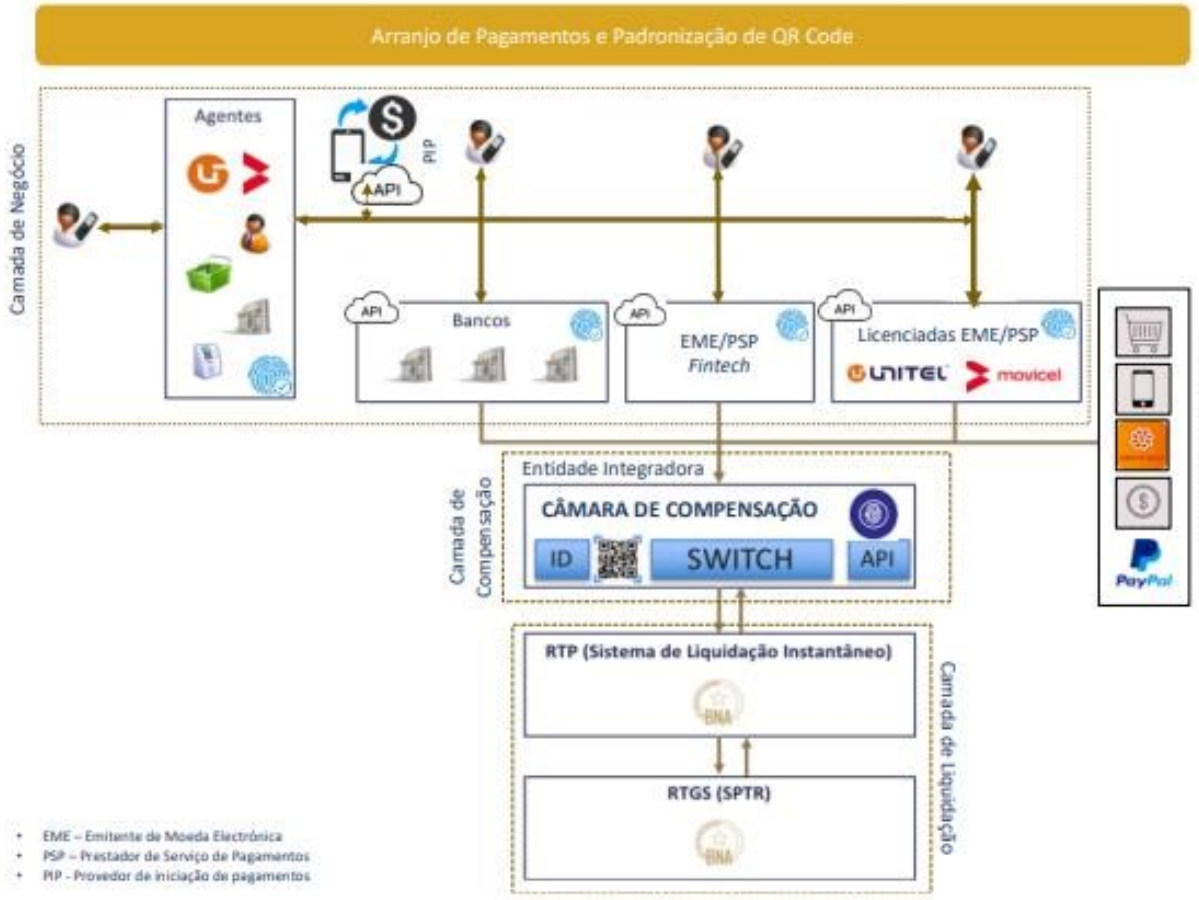
"Existindo já uma rede de telecomunicações móveis bastante consolidada no mercado angolano, o Banco Nacional de Angola pretende implementar um Sistema de Transferências Móveis e Instantâneas (STMI), que esteja disponível em todo o território angolano e acessível a toda população, vulgarmente conhecido como Mobile Money", justifica o regulador no seu site.

A abertura dos pedidos de informação destina-se à elaboração de um pedido de proposta (RFP) para escolha do operador tecnológico da entidade que será responsável pela gestão tecnológica do STMI, que terá de ser uma sociedade operadora de sistema de pagamentos sediada em Angola. O sistema de pagamentos em Angola assenta atualmente na utilização de quatro instrumentos de pagamentos escriturais (cheques, cartões de pagamento, transferências a crédito e débitos diretos) e é composto por quatro subsistemas interbancários, um sistema de pagamentos de grandes montantes e um subsistema de liquidação de títulos.

https://www.angonoticias.com/Artigos/item/64604/bna-quer-implementar-sistema-de-dinheiro-digital-no-pais

A. Aspectos Funcionais e técnicos

A figura abaixo ilustra a arquitetura funcional do STMI.



1. Camada de negócio:

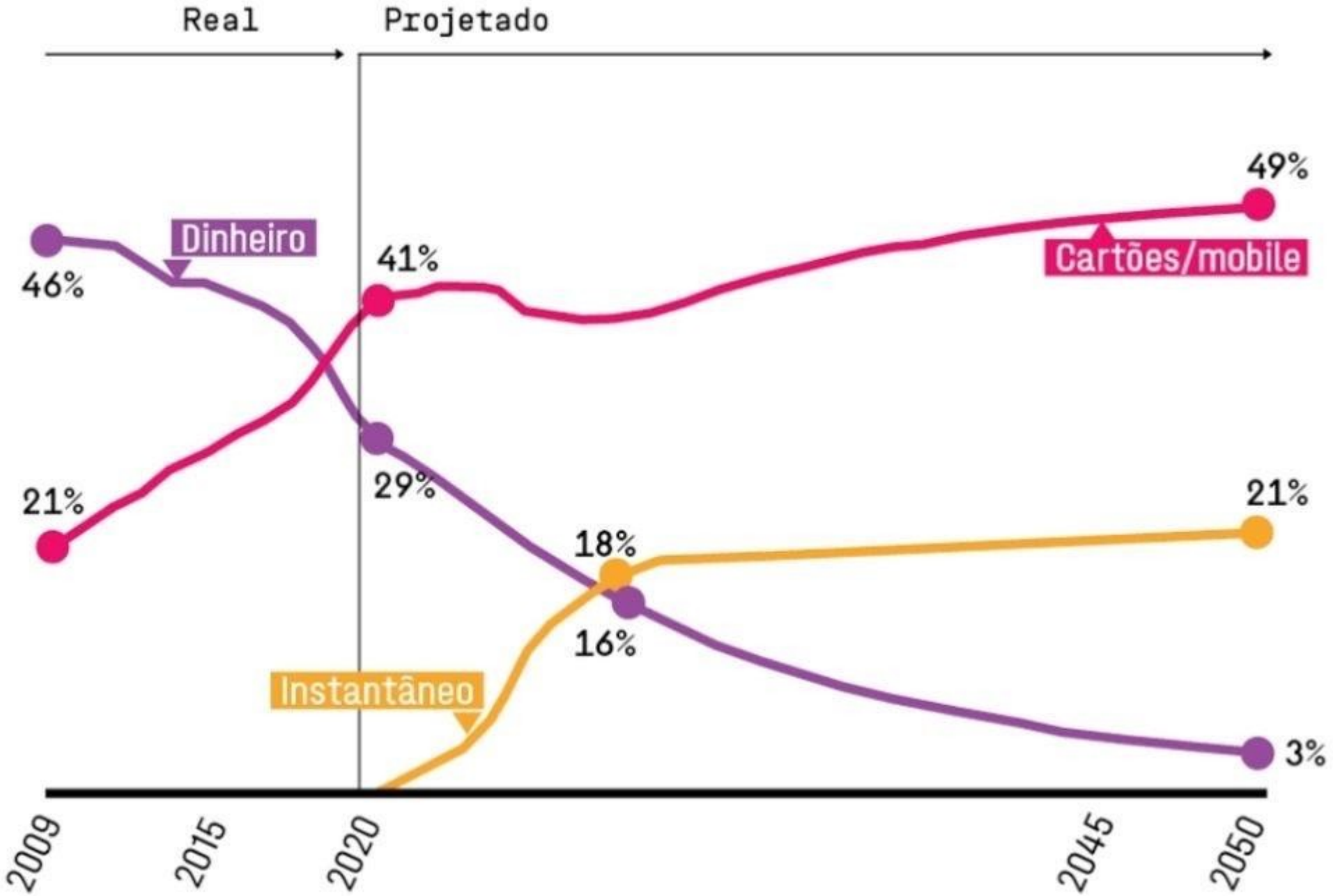
- Definição de regras, normas e procedimentos
- Operacionalização dos serviços
- Desenvolvimento do negócio

2. Camada de compensação:

- Regras, normas e procedimentos de compensação
- Identificação do pagamento
- Serviço de endereços
- Switch
- Framework API para integrações
- Framework QR Code
- E-KYC

3. Camada liquidação:

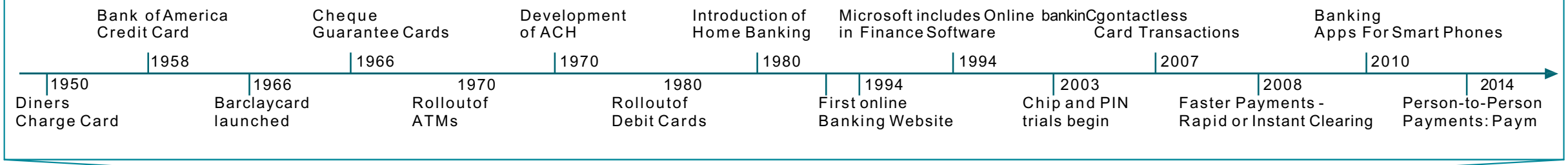
- Regras, normas e procedimentos de liquidação
- RTP
- SPTR


Real
Projetado
Dinheiro
Cartões/mobile
Instantâneo
46%
41%
49%
29%
21%
21%
18%
16%
3%
2009
2015
2020
2045
2050

PANORAMA DAS FRAUDES

RISCOS DE SEGURANÇA DE TI

Desenvolvimento de produtos bancários



Evolução das vulnerabilidades para as fraudes

Riscos de Fraude

Risk Management
- Credit Risk
- Market Risk
- Operational Risk
- Financial Crime
- Conduct

Historic separation of Domains

Cheque Fraud

Lost and Stolen Cards

Application Fraud

Mail Non-Receipt Fraud

Counterfeit Card Fraud

Cash Machine / ATM Fraud

Evolving Product, Business and IT risks driving the integration of Risk and IT

Integração dos Riscos e TI

Account Take-over

Social Engineering

Card Not Present Fraud

Phone Banking Fraud

Fake Banking Apps

Phishing Websites

Industry responses eg: Chip & Pin, EMV, 3-D Secure

Technology responses eg: Data analytics, Sophisticated profiling

Riscos de Segurança de TI

IT Security
- Policies
- Physical Controls
- Anti-virus
- Access Controls
- Device Hardening
- Segmentation

Advanced Persistent Threats

Resilience

Remote Access Trojans

Key logging

HTML injection

Drive by Downloads

Man-in-the Browser Attacks

Disaster Recovery

Intrusion

Screen capturing

Man-in-the-Middle Attacks

Bring Your Own Device

Distributed Denial of Service

Proxy servers, DNS poisoning

Evolução da TI

Mainframe | Mini | Client - Server | Web Services | Cloud

portaldeti.com/pt/noticias/item/318-startup-zambiana-lanca-rede-de-fintechs-africanas

STARTUPS

Startup zambiana lança rede de fintechs africanas

By Joaquim Cassicato agosto 17, 2020

Imagem: D.R

A Startup zambiana denominada Zazu, lançou uma plataforma para agregar as fintechs e facilitar pagamentos em tempo real em toda a África.

Nos primeiros meses da sua criação em 2015, a Zazu permitia que agricultores com produtos extras se os, tendo evoluído para o espaço de banco digital em 2017. A sua carteira

portaldeti.com/pt/noticias/item/302-m-pesa-lidera-mercado-de-servico-financeiro-movel-em-africa

E-BUSINESS

M-Pesa lidera mercado de serviço financeiro móvel em África

By Joaquim Cassicato agosto 10, 2020

A plataforma de serviço financeiro móvel M-Pesa, está agora a processar transacções na ordem dos Sh1.6 trilhões (cerca de **14,7 bilhões de dólares**) por mês no Quénia e em outros países africanos.

Imagem: D.R

E quem são os principais varejistas online no Brasil?

TOP 10 WEB DOMAINS

	TOTAL DIGITAL POPULATION	DESKTOP	MOBILE	APPS
1	AMERICANAS.COM.BR	AMERICANAS.COM.BR	AMERICANAS.COM.BR	AMERICANAS.COM.BR
2	MERCADOLIVRE.COM.BR	MERCADOLIVRE.COM.BR	MERCADOLIVRE.COM.BR	**IFOOD.COM.BR**
3	MAGAZINELUIZA.COM.BR	MAGAZINELUIZA.COM.BR	MAGAZINELUIZA.COM.BR	MERCADOLIBRE.COM
4	MERCADOLIBRE.COM	MERCADOLIBRE.COM	MERCADOLIBRE.COM	MOTOROLA.COM
5	IFOOD.COM.BR	IFOOD.COM.BR	IFOOD.COM.BR	MAGAZINELUIZA.COM.BR
6	CASASBAHIA.COM.BR	CASASBAHIA.COM.BR	CASASBAHIA.COM.BR	**WISH.COM**
7	SUBMARINO.COM.BR	SUBMARINO.COM.BR	SUBMARINO.COM.BR	**UBEREATS.COM**
8	MOTOROLA.COM	MOTOROLA.COM	MOTOROLA.COM	**ALIEXPRESS.COM**
9	SHOPTIME.COM.BR	SHOPTIME.COM.BR	SHOPTIME.COM.BR	**SHOPEE.COM.BR**
10	AMAZON.COM.BR	AMAZON.COM.BR	AMAZON.COM.BR	SUBMARINO.COM.BR

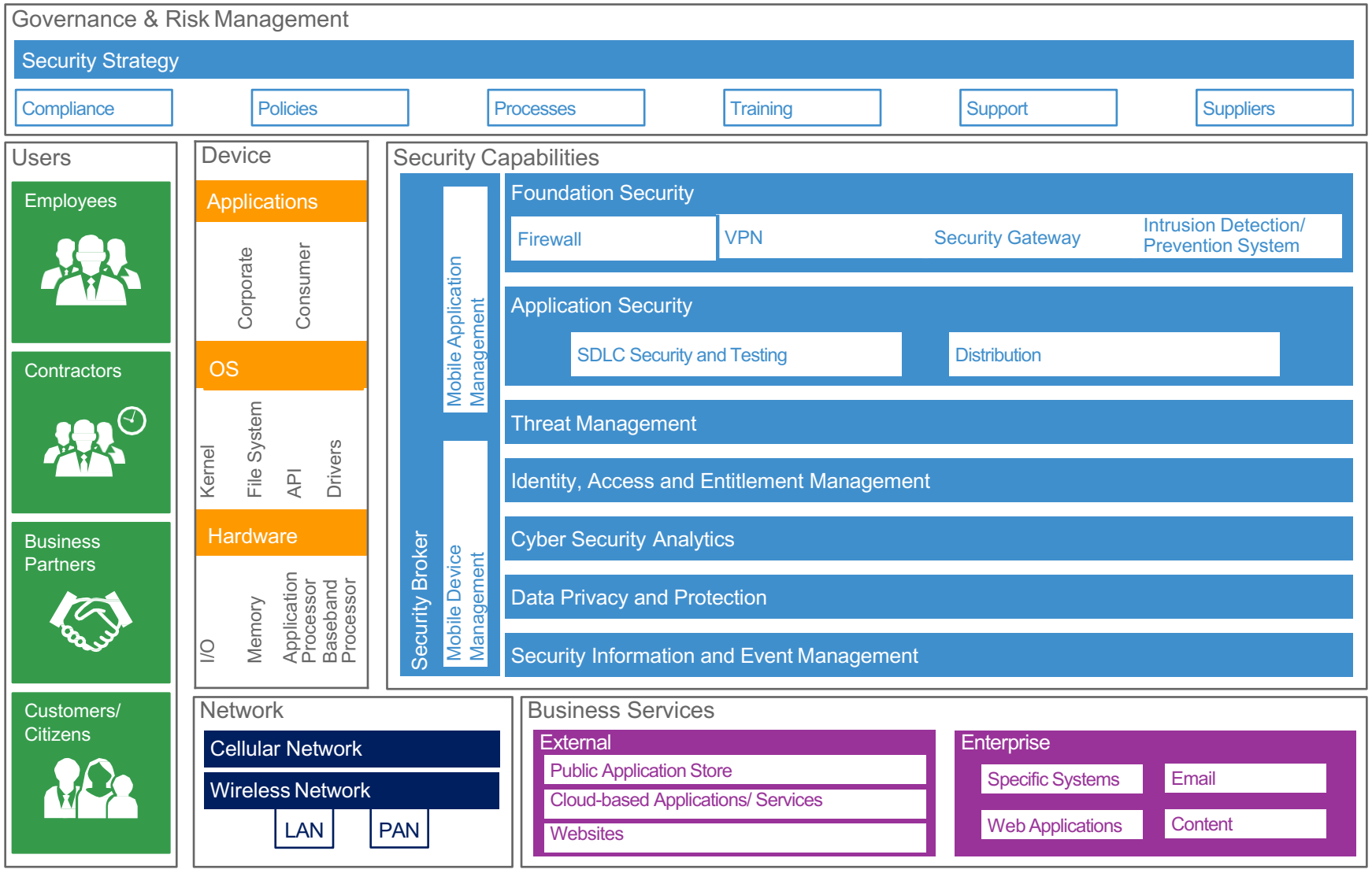
Comscore MMX MP Brasil - Abril 2020 - Brasil.

iFood lança cartão pré-pago e conta digital para restaurantes parceiros

Serviços poderão ser utilizados para obtenção de crédito e realização de pagamentos.

O grupo Movile, responsável pelas atividades do iFood e de outras startups brasileiras, anunciou a criação de um cartão pré-pago para os restaurantes associados ao serviço de entregas. O iFood Facilita, como foi chamado, inclui bandeira Visa e será atrelado a uma conta digital, possibilitando a realização de saques, transferências e pagamentos.

Mobile Security Reference Architecture



The Anatomy Of A Mobile Attack

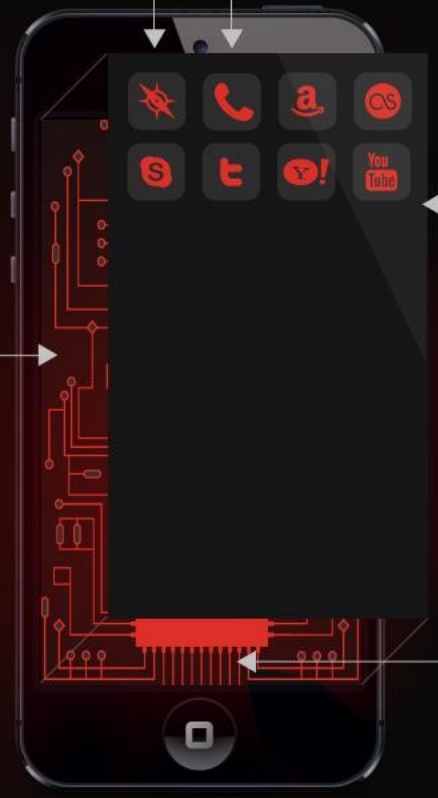
Attack Surface: Device

BROWSER

Phishing
Framing
Clickjacking
Man-in-the-Middle
Buffer Overflow
Data Caching

PHONE / SMS

Baseband Attacks
SMishing



APPS

Sensitive Data Storage
No Encryption/ Weak Encryption
Improper SSL Validation
Config Manipulation
Dynamic Runtime Injection
Unintended Permissions
Escalated Privileges

SYSTEM

No Passcode/Weak Passcode
iOS Jailbreaking
Android Rootng
OS Data Caching
Passwords & Data Accessible
Carrier-Loaded Software
No Encryption/Weak Encryption
User-Initiated Code

MALWARE

THE INTERNET

Attack Surface: Network

Wi-Fi (No Encryption/Weak Encryption)
Rogue Access Point
Packet Sniffing
Man-in-the-Middle (MITM)
Session Hijacking
DNS Poisoning
SSLStrip
Fake SSL Certificate

Attack Surface: Data Center

WEB SERVER

Platform Vulnerabilities
Server Misconfiguration
Cross-site Scripting (XSS)
Cross-Site Request Forgery (CSRF)
Weak Input Validation
Brute Force Attacks

DATABASE

SQL Injection
Privilege Escalation
Data Dumping
OS Command Execution

VIAFORENSICS

APPS DE BANCOS PARA IOS PODEM EXPOR DADOS DE USUÁRIOS

As versões de aplicativos de seis bancos para iOS apresentam brechas que podem deixar informações de usuários expostas.

Quem afirma isso é o especialista em segurança Renato Ribeiro, que testou apps de dez instituições financeiras e encontrou falhas nos desenvolvidos por Banco do Brasil, Caixa, Banco do Nordeste, HSBC, Citibank e Bradesco. Todos eles, porém, negaram a existência de problemas.

HTTP://EXAME.ABRIL.COM.BR/TECNOLOGIA/NOTICIAS/APPS-DE-BANCOS-PARA-IOS-PODEM-EXPOR-DADOS-DE-USUARIOS

As regras do BNA para Segurança Cibernética

O Aviso 08/2020 foi estabelecido pelo Banco Nacional de Angola(BNA) em Março de 2020, com o objectivo de definir Regras e Ações a serem tomadas pelas Instituições Financeiras sobre os serviços baseados em Computação na Nuvem.

- Plano de Continuidade de Negócios: testes de cenários de incidentes de segurança cibernética e atualização do BIA (análise de impacto aos negócios).
- Estabelecer uma matriz de risco cibernético para classificação dos incidentes de segurança da informação.
- Revisão e atualização da Política, Norma e Procedimentos de resposta a incidentes de segurança da informação.
- Definir o processo de comunicação, ao BNA, sobre as violações das redes e dossistemas de informação ou perdas de integridade com impacto significativo no funcionamento das referidas redes e serviços;

QUAIS SÃO OS PRINCIPAIS CONTROLES?

É importante destacar que, no que diz respeito aos procedimentos e controles de Cibersegurança exigidos pelo Aviso, o BNA entende que eles devem incluir no mínimo os seguintes 9 (nove) requisitos.

1. Autenticação;
2. Criptografia;
3. Prevenção e detecção de intrusão;
4. Prevenção de vazamento de informações;
5. Realização periódica de testes e varreduras para detecção de vulnerabilidades;
6. Proteção contra softwares maliciosos;
7. Mecanismos de rastreabilidade;
8. Controles de acesso e de segmentação da rede de computadores;
9. Manutenção de cópias de segurança dos dados e das informações.

Evolução das nossas capacidades de Segurança Cibernética em conformidade com o Aviso 08/2020 do BNA

Segurança na Aplicação

Identificação de ameaças e vulnerabilidades no design, desenvolvimento, implantação, atualização das aplicações do banco.

Auditoria & Compliance

Políticas e procedimentos, regulamentos, auditorias internas e externas, controle de conformidade.

Plano de Continuidade de Negócios (PCN)

Política do PCN, análise de impacto, abordagem de recuperação de desastres, mecanismos de tolerância a falhas / failover.

Cloud Hardening

Proteção do ambiente de cloud e redução de vulnerabilidades.

Criptografia e Tokenization

Proteção dos dados em trânsito, dados em uso, dados em repouso.

Governança de Segurança da Informação

Governança da Segurança da Informação em Cloud, Treinamentos sobre Segurança da Informação e Campanhas de Conscientização.

Gestão de Identidades e Acessos

Segurança de recursos humanos, Restrição / Autorização de Acesso de Utilizador, Revisão de Acesso do Utilizador, Autenticação, Gestão de Senhas.

Proteção de dados

Classificação de dados, backup de dados, avaliações de risco, segregação de dados, política de retenção, fuga de informações e descarte seguro.

Operação de Infraestrutura

Documentação do sistema, planejamento de capacidade / recursos, gestão de alterações, problemas e configurações.

Interoperabilidade

Capacidade do banco de usar o mesmo conjunto de ferramentas, imagens de servidor, aplicações com uma variedade de fornecedores e plataformas de computação em nuvem.

Jurídico

Acordos de confidencialidade, acordos com terceiros, preparação jurídica para resposta a incidentes, suporte a Política de Segurança da Informação em Justiça Criminal, Licenciamento e Direitos de Propriedade Intelectual

Configuração de Rede

Segmentação / segregação, redes compartilhadas, suporte a redes privadas virtuais, ambientes de produção / não produção.

Segurança física

Política de segurança física, vigilância, acesso do utilizador, autorização de área segura e entrada de pessoas não autorizadas, gestão de ativos.

Portabilidade

Capacidade de mover as aplicações e dados entre um fornecedor de cloud e outro e de se mover entre diferentes ambientes de cloud (públicas, privadas e híbridas)

Segurança da Informação e Gestão de Eventos

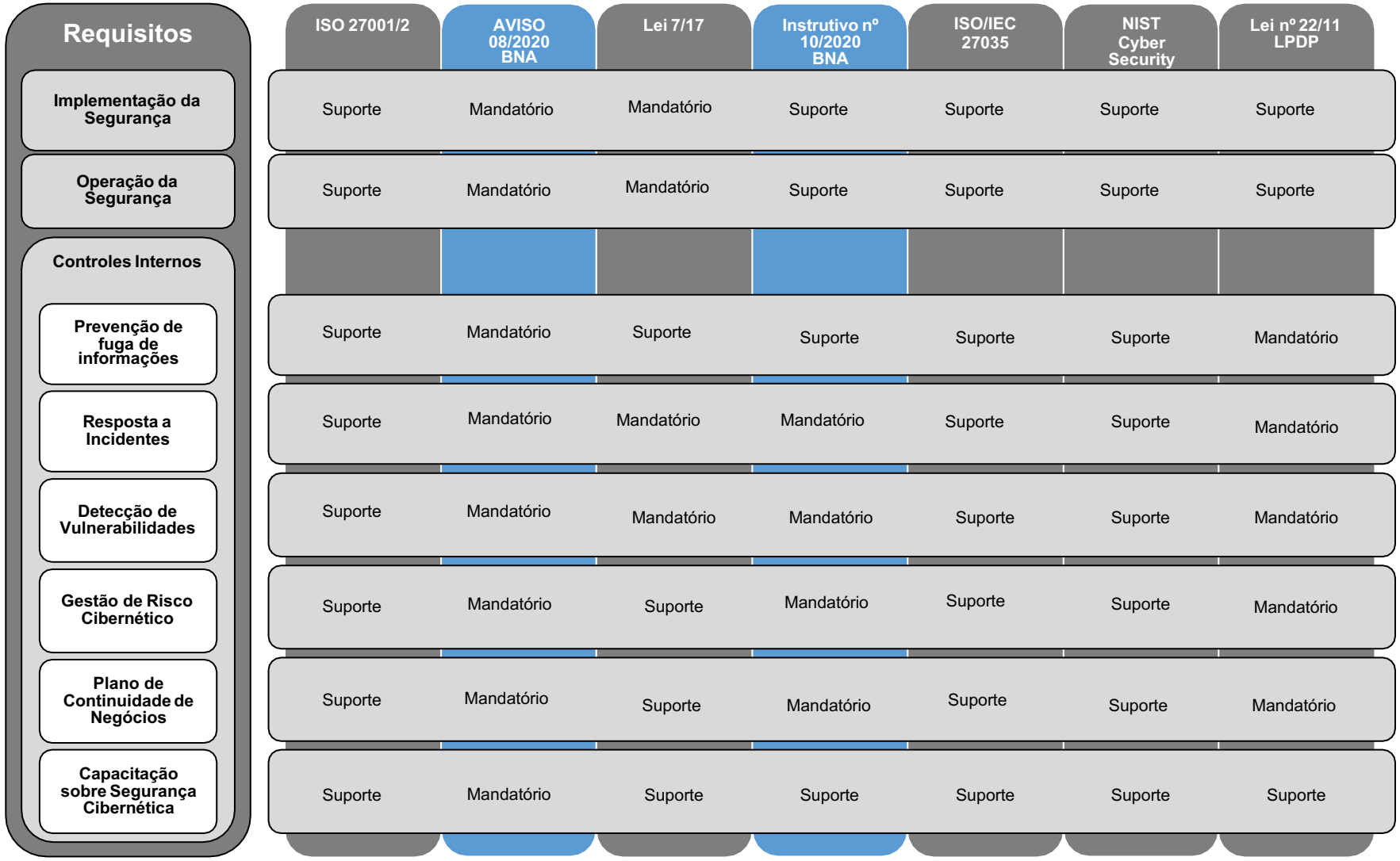
Detecção / Prevenção de Intrusão, Métricas de Resposta a Incidentes, Gestão de Incidentes e Logs.

Gestão de Vulnerabilidades

Avaliação de vulnerabilidades, suporte a testes de penetração, gestão de patches, antivírus e anti-malware.

Demais Gabinetes

Diversas leis, regulamentos e normas locais e internacionais, requerem testes e controles internos de Segurança Cibernética.




Cyber Security
O que está por vir!

Google, Facebook, Amazon e cia NÃO estão oferecendo serviços bancários, então pare de dizer que estão!

Segundo Chris Skinner, que é conhecido como a pessoa mais influente em tecnologia no Reino Unido, as big techs estão estão a fazer parcerias com grandes bancos para oferecer um pouco mais de facilidade financeira, e não contas bancárias. No último mês houve uma onda de anúncios do Facebook, Apple, Google e Amazon sobre questões bancárias. Vimos as principais atividades do Facebook na tentativa de criar uma moeda digital chamada libra, e a Apple se direcionou para o setor financeiro com um cartão de crédito do Goldman Sachs que, em apenas um mês, ofereceu uma linha de crédito de US$ 10 bilhões. O Google fez uma parceria com o Citi para oferecer uma conta de depósito, assim como fez a Amazon com o J.P. Morgan Chase.

O resultado é um frenesi da cobertura da mídia com o foco sobre a grande mudança das big techs para o setor bancário. Minha opinião sobre isso foi publicada várias vezes, mais recentemente dizendo que as big techs só podem entrar no setor bancário junto com os grandes bancos.

https://noomis.febraban.org.br/especialista/chris-skinner/google-facebook-amazon-e-cia-nao-estao-oferecendo-servicos-bancarios-entao-pare-de-dizer-que-estao

O presidente da Associação Portuguesa de Bancos (APB), Fernando Faria de Oliveira, alertou esta terça-feira para a ameaça das grandes plataformas digitais, como a Google, Amazon, Facebook e Apple ao negócio bancário.

"A grande ameaça ao setor bancário surge não das 'startups' fintech — onde o caminho tem sido, acima de tudo, de cooperação — mas dos operadores das grandes plataformas digitais, os designados GAFA (Google, Amazon, Facebook, Apple), todos eles entidades não europeias", disse.

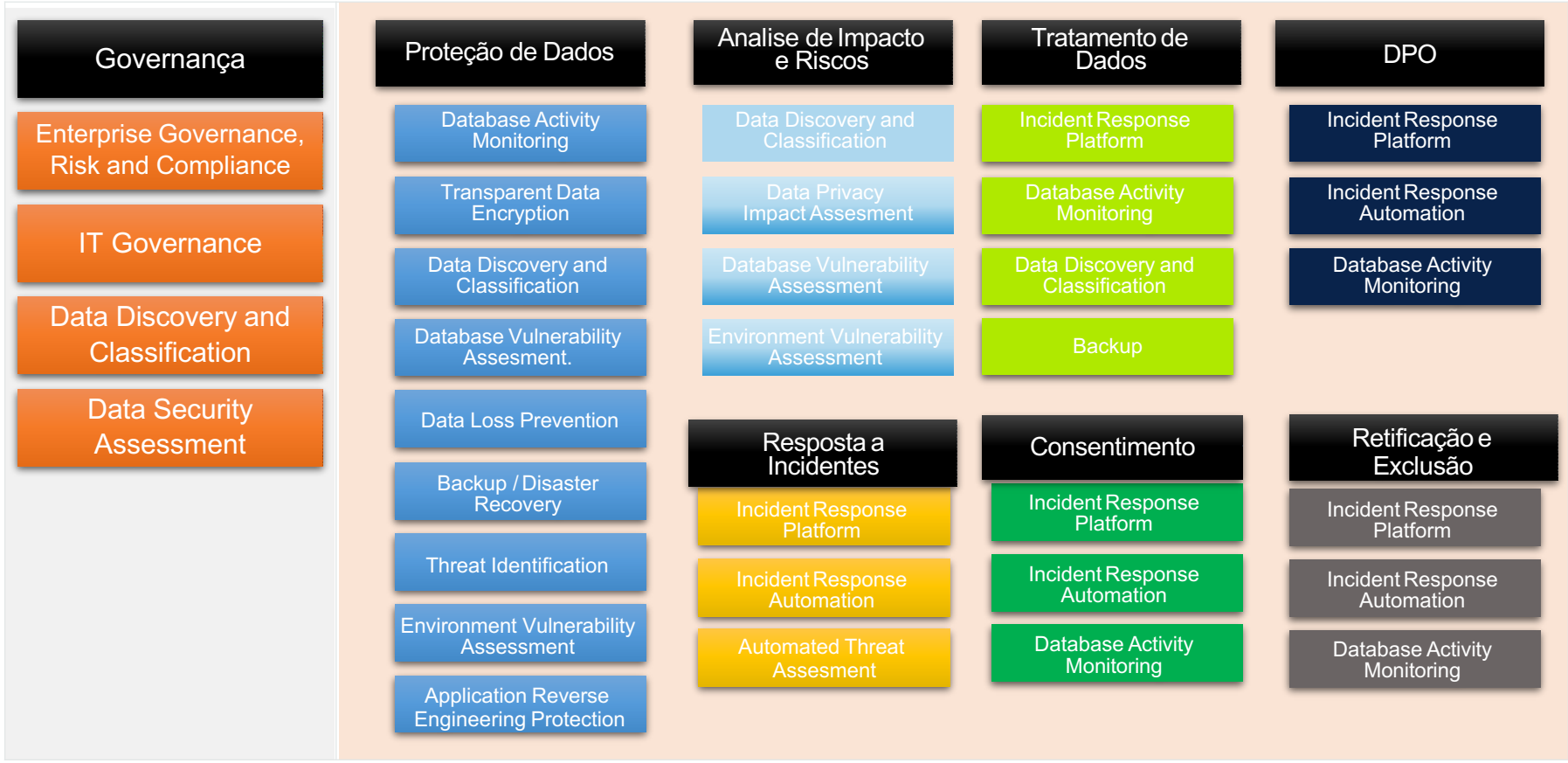
O responsável falava na abertura da conferência "Supervisão comportamental bancária — Novos desafios dez anos depois da crise financeira", promovida pelo Banco de Portugal, que decorre hoje em Lisboa.

"Estas entidades possuem muita informação sobre os clientes, o que lhes permite oferecer e produtos 'tailormade' [feitos à medida], de uma forma que, no limite, exclui os restantes operadores, incluindo os prestadores de serviços financeiros incumbente", avisou.

Faria de Oliveira abordou, por isso, a importância de todos os operadores obedecerem a um quadro legal e regulatório, designadamente em termos de proteção do consumidor.

https://24.sapo.pt/atualidade/artigos/google-amazon-facebook-e-apple-sao-a-grande-ameaca-ao-negocio-bancario

Arquitetura de Tecnologia e a Lei Geral de Proteção de Dados



Estabelecer uma estrutura de Governança de Privacidade de Dados, integrada à Governança Corporativa: Art. 3º, Art. 7º, Art. 8º, Art. 9º, Art. 10º, Art. 12º, Art. 14º, Art. 15º, Art. 41º, Art. 42º, Art. 46º, Art. 49º, Art. 50º

Assegurar a proteção dos dados contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração e comunicação inadequada ou ilícita, mesmo após o término do contrato: Art. 6º, Art. 8º, Art. 9º, Art. 11º, Art. 12º, Art. 33º, Art. 34º, Art. 35º, Art. 36º

Realizar Avaliações periódicas de Riscos e Impactos à Privacidade dos Dados: Art. 10º, Art. 52º, Art. 53º, Art. 54º

Atender as solicitações do Titular e Órgão Competente quanto as informações referentes ao tratamento dos dados: Art. 18º, Art. 19º, Art. 22º, Art. 37º, Art. 38º, Art. 40º, Art. 41º, Art. 48º

Assegurar que o Operador realize o tratamento segundo as instruções Estabelecidas: Art. 18º, Art. 19º, Art. 21º, Art. 51º

Gerenciar e Responder a Incidentes (próprios e dos operadores): Art. 42º, Art. 43º, Art. 44º, Art. 45º

Assegurar que o tratamento do dados ocorra exclusivamente aos propósitos acordados no Consentimento fornecido pelo Titular: Art. 11º, Art. 12º, Art. 19º, Art. 21º, Art. 38º, Art. 39º, Art. 47º

Assegurar que os dados são bloqueados / excluídos quando necessários (exemplo: a pedido do Titular, ao término do contrato): Art. 16º

Arquitetura de referência: LGPD vs Capacidades (1/2)

Domínio	Capacidade	Artigos LGPD	Requisitos Tecnológicos
Governança	Estabelecer uma estrutura de Governança de Privacidade de Dados, integrada à Governança Corporativa	Art. 3º, Art. 7º, Art. 8º, Art. 9º, Art. 10º, Art. 12º, Art. 14º, Art. 15º, Art. 41º, Art. 42º, Art. 46º, Art. 49º, Art. 50º	-Enterprise Governance, Risk and Compliance - IT Governance -Data Discovery and Classification - Data Security Assessment
Proteção de Dados	Assegurar a proteção dos dados contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração e comunicação inadequada ou ilícita, mesmo após o término do contrato.	Art. 6º, Art. 8º, Art. 9º, Art. 11º, Art. 12º, Art. 33º, Art. 34º, Art. 35º, Art. 36º	- Database Activity Monitoring - Transparent Data Encryption -Data Discovery and Classification -Database Vulnerability Assesment - Data Loss Prevention - Backup / Disaster Recovery - Threat Identification -Environment Vulnerability Assessment -Application Reverse Engineering Protection
Resposta a Incidentes	Gerenciar e Responder a Incidentes (próprios e dos operadores)	Art. 42º, Art. 43º, Art. 44º, Art. 45º	- Incident Response Platform -Incident Response Automation -Automated Threat Assesment
Analise de Impacto e Riscos	Realizar Avaliações periódicas de Riscos e Impactos à Privacidade dos Dados	Art. 10º, Art. 52º, Art. 53º, Art. 54º	- Data Discovery and Classification -Data Privacy Impact Assesment -Database Vulnerability Assessment -Environment Vulnerability Assessment

Arquitetura de referência: LGPD vs Capacidades (2/2)

Domínio	Capacidade	Artigos LGPD	Requisitos Tecnológicos
DPO	Assegurar que o Operador realize o tratamento segundo as instruções Estabelecidas.	Art. 18º, Art. 19º, Art. 21º, Art. 51º	- Incident Response Platform - Incident Response Automation -Database Activity Monitoring
Tratamento de Dados	Atender as solicitações do Titular e Órgão Competente quanto as informações referentes ao tratamento dos dados.	Art. 18º, Art. 19º, Art. 22º, Art. 37º, Art. 38º, Art. 40º, Art. 41º, Art. 48º	-Database Activity Monitoring -Transparent Data Encryption -Data Discovery and Classification -Database Vulnerability Assesment - Data Loss Prevention - Backup / Disaster Recovery - Threat Identification -Environment Vulnerability Assessment -Application Reverse Engineering Protection
Consentimento	Assegurar que o tratamento do dados ocorra exclusivamente aos propósitos acordados no Consentimento fornecido pelo Titular	Art. 11º, Art. 12º, Art. 19º, Art. 21º, Art. 38º, Art. 39º, Art. 47º	- Incident Response Platform -Incident Response Automation -Database Activity Monitoring
Retificação e Exclusão	Assegurar que os dados são bloqueados / excluídos quando necessários (exemplo: a pedido do Titular, ao término do contrato)	Art. 16º	- Incident Response Platform -Incident Response Automation -Database Activity Monitoring

Estratégia de Governança de Dados e Segurança da Informação

Privacidade, política, risco e compliance | Arquitetura de Governança e Segurança | Gestão do Plano de Continuidade dos Negócios

Gerenciamento de vulnerabilidades | Analítico e Monitoramento | Gestão de Incidentes de Segurança | Defesa preventiva

Origem

Plataforma de Big Data

Usuários

Captura dos dados	Processamento e Armazenamento			Acesso a dados
Criptografia de rede	Standard Operating Environment	Operating Platform Hardening		Criptografia de rede
Gerenciamento de credencial	Virtualization Security	Gestão do Servidor		Gerenciamento de credencial
Gerenciamento de sessão	Autenticação do usuário	Autenticação da aplicação		Gerenciamento de sessão
Autenticação do usuário	Coarse-Grained Authorization	Fine-Grained Authorization		Autenticação do usuário
Single Sign-On	Criptografia de Arquivos	Database Block Encryption	Data Element Encryption	Single Sign-On
Autenticação da aplicação	Controle de Acesso aos Dados	Secure Data Destruction	Classificação da informação	Autenticação da aplicação
Mascaramento de dados				Mascaramento de dados
Web App Security				Web App Security
Custom App Security				Custom App Security

Serviços de suporte

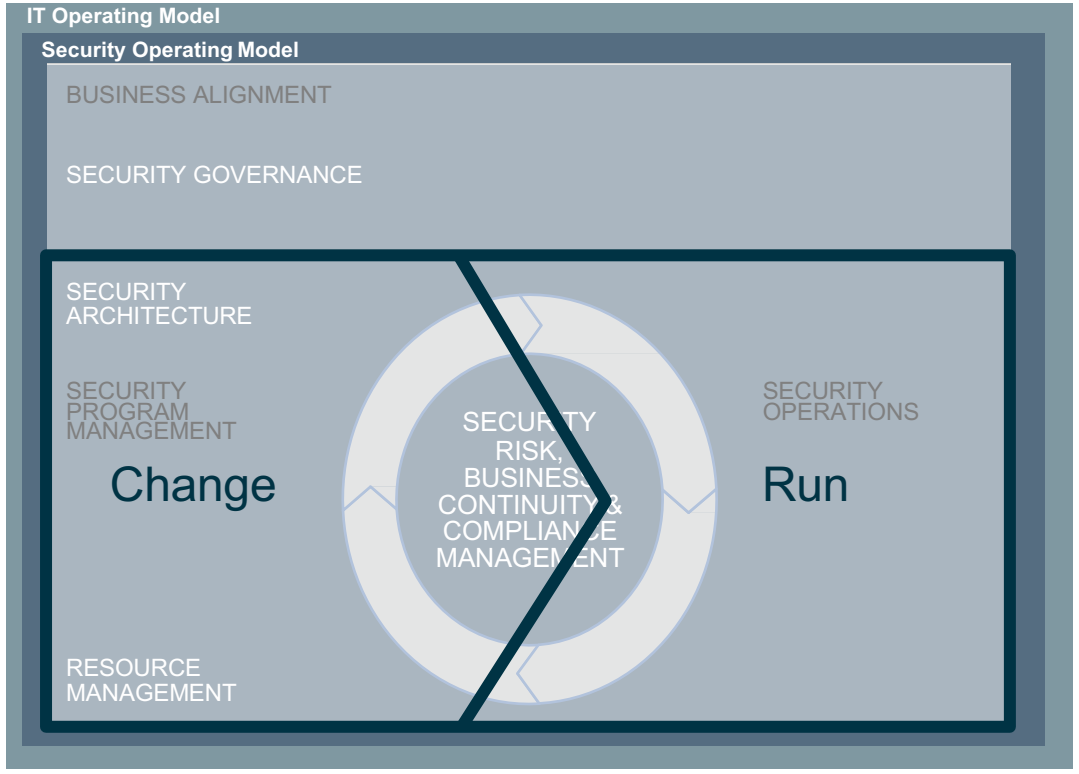
Gerenciamento de identidade e acessos | Infraestrutura de segurança | Proteção dos dados

Gerenciamento de identidade e acessos | Infraestrutura de segurança | Proteção de dados | Segurança da aplicação | Estratégia de Segurança | Cyber Security

Gerencie a complexidade da Cibersegurança

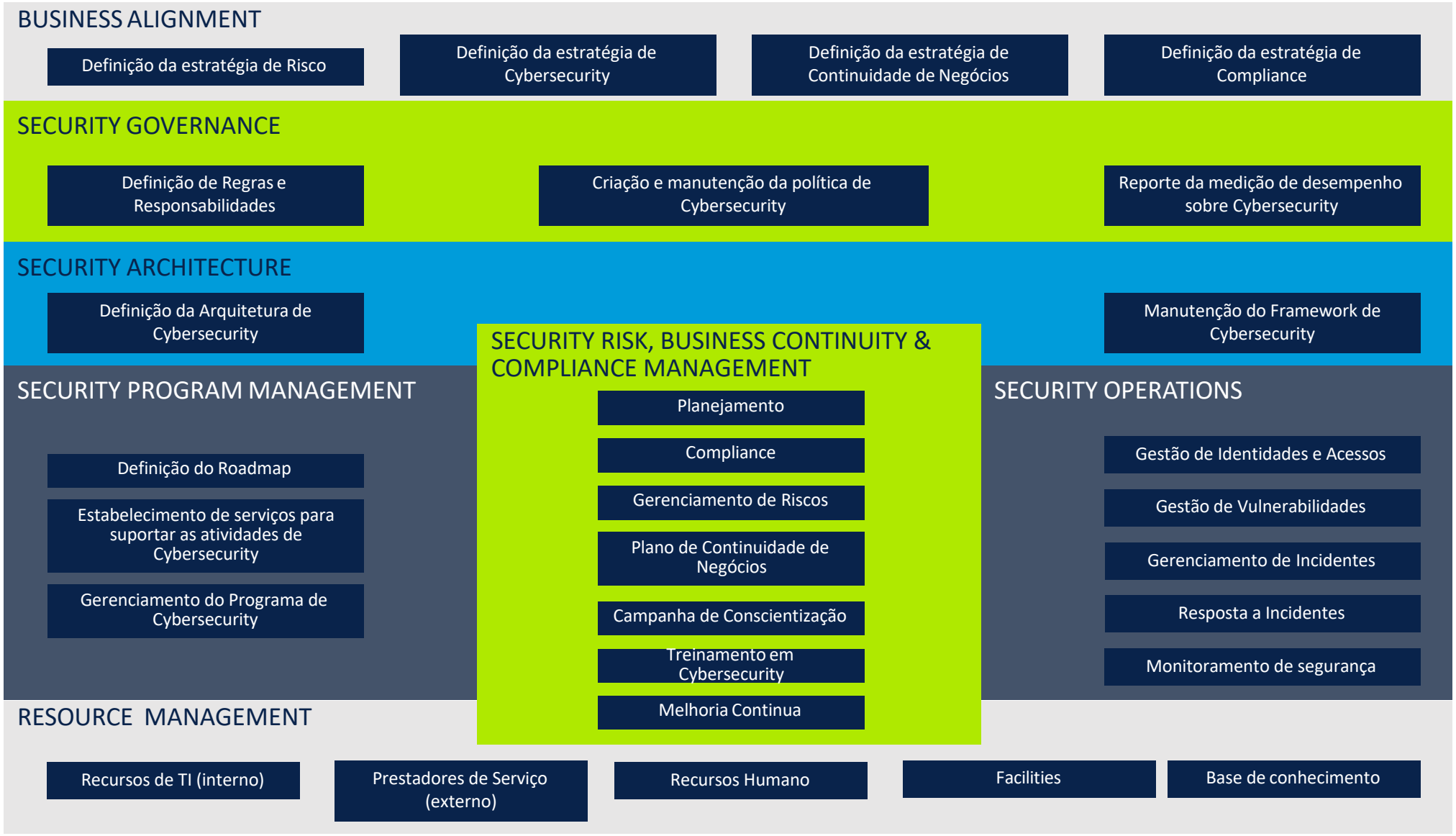
Estabeleça um programa de cibersegurança de ponta a ponta e integre-o aos processos de arquitetura corporativa existentes para reduzir os níveis de complexidade e produzir resultados avaliados pelos negócios.

Visão geral dos componentes do Modelo Operacional de Cybersecurity da SpeedNet



- Estabeleça uma nova visão de como a cibersegurança se integra e trabalha com a TI e os negócios, criando efetivamente um modelo operacional de cibersegurança.
- Estabeleça operações básicas de cibersegurança em várias funções organizacionais (funções, processos, métricas e políticas de governança).
- Desenvolva um modelo de processo de tecnologia de cibersegurança e crie a base do investimento em cibersegurança com base nos requisitos de negócios.
- Integre-se à arquitetura, tecnologia e processos gerais da instituição.

Modelo Operacional de Cybersecurity da SpeedNet



Hora de modernizar a segurança cibernética

- As Arquiteturas de Segurança tradicionais precisam evoluir para Arquiteturas com recursos de serviços em nuvem, tais como: secure web gateway, cloud access security broker, firewall-as-a-service e zero-trust network access.

- Estabeleça processos e tecnologias para Big Data e Governança de Dados, principalmente controles internos baseados em HSM para criptografia dos dados sensíveis e atendimento aos requisitos de compliance.

- Implemente a estratégia Shift Left de Segurança Cibernética no processo de Desenvolvimento de Software, incluindo capacidades de DevSecOps e Penetration Tests automatizados.

- Defina a estratégia de prevenção à fraudes alinhada com as atividades de “inteligência em segurança cibernética”. Ou seja, à organização deve realizar a Orquestração das capacidades de segurança, alinhada a gestão de risco e prevenção à fraudes.

Obrigado!

Gabinete de Cyber Sec. e Transformação Digital
Denny.roger@speednet.co.ao
Bruno.laureano@speednet.co.ao

Direção de Negócios
Dario.miguel@speednet.co.ao

LIGA-TE AO MUNDO

TRANQUILAMENTE!

TELECOMUNICAÇÕES, IT, CONSULTORIA

www.speednet.co.ao
geral@speednet.co.ao
Tel.: +244 938 882 171
Rua das Travessas, Travessa nº3, Casa 18, Talatona, Belas
Luanda/ Angola