DANDO VIDA A
POLÍTICAS
INTELIGENTES

CIBERSEGURANÇA PARA INCLUSÃO FINANCEIRA: GUIA DE FRAMEWORK E RISCOS

Nota Orientadora Nº 37
Outubro de 2019

NOTA ORIENTADORA

ÍNDICE

CONFIRMAÇÕES

A AFI expressa seus agradecimentos ao presidente do subgrupo de cibersegurança, Komitas Stepanyan, do Banco Central da Armênia, por sua excelente liderança. Também gostaríamos de agradecer aos seguintes países membros que contribuíram para o trabalho: Banco de Gana; Banco Al-Maghrib; Banco Central da Nigéria; Banco da Namíbia; Banco Central do Sudão e Banco da Reserva de Fiji. A AFI também agradece a Paul Makin por ajudar o subgrupo a realizar pesquisas relevantes e redigir o documento.

A AFI também reconhece e aprecia os parceiros privados, especialistas e stakeholders que contribuíram para o documento. Entre eles estão o Banco Central Europeu, GSMA, Mastercard, Visa, FMI, UIT, CGAP e o Fórum Económico Mundial.

Ali Ghiyazuddin Mohammad e Kennedy Komba, da unidade de gestão da AFI, também forneceram contribuições e comentários para os framework.

O fluxo de trabalho de serviços financeiros digitais é apoiado pelos Parceiros de Financiamento da AFI.

1 INTRODUÇÃO

1.1 CONTEXTO

Nos últimos anos, os reguladores e supervisores do setor financeiro tornaram-se cada vez mais conscientes de que os serviços financeiros visavam abordar a inclusão financeira (FI) Os desafios em todo o mundo estão a tornar-se vulneráveis a ciberameaças, principalmente devido ao papel crescente dos serviços digitais (incluindo tecnologias móveis e outras) na prestação de serviços financeiros.

À medida que os serviços financeiros se tornam cada vez mais digitalizados, o volume de dados digitais sensíveis cresce exponencialmente e, como consequência, o potencial de impactos pessoais e no sistema causados por violações de dados. Como tal, a necessidade de salvaguardas
a partir do acesso ilícito a esses dados torna-se cada vez mais importante.

No curso da implementação de seu papel facilitador e de coordenação para melhorar a inclusão financeira por meio da alavancagem de serviços financeiros digitais direcionados aos consumidores desbancarizados e sem sofisticação, os membros da AFI perceberam que precisam de orientação específica para lidar com os riscos de cibersegurança do lado da demanda. Também são necessárias perspetivas do lado da oferta com foco na peculiaridade das provisões de serviços financeiros direcionadas ao segmento inferior da pirâmide. A este respeito, o Grupo de Trabalho de Serviços Financeiros Digitais (SFDs) da AFI criou um subgrupo sobre cibersegurança para apurar os riscos de cibersegurança à luz do digital.
Inovações FinTech. Além disso, o subgrupo também fornecerá recomendações de políticas para monitorizar, identificar, gerir e mitigar riscos de cibersegurança, incluindo o desenvolvimento de um Guia de Riscos de Cibersegurança, ou seja, este documento.

1.2 GUIA DE RISCO DE CIBESEGURANÇA

1.2.1 PROPÓSITO

O principal objetivo deste documento é fornecer princípios fundamentais e melhores práticas que oferecerão orientação para ajudar as autoridades reguladoras e de supervisão na criação de ferramentas para o setor financeiro lidar com os riscos de cibersegurança. O Guia também é útil para os prestadores de serviços financeiros para ajudá-los a fortalecer sua gestão de riscos cibernéticos na prestação de serviços financeiros que visam os consumidores de última milha e desassistidos na base da pirâmide.

1.2.2 METODOLOGIA

O desenvolvimento deste Guia de Riscos envolveu o seguinte:

- Entrevistas com stakeholders, incluindo membros da AFI ativos em cibersegurança, esquemas de pagamento internacionais, autoridades reguladoras supranacionais, desenvolvedores de outros frameworks de cibersegurança e especialistas independentes do setor.
- Meta-análise dos frameworks existentes, com foco específico naqueles destacados pelos stakeholders.
- Desenvolvimento de um modelo genérico de pagamentos digitais e serviços financeiros com um componente significativo de inclusão financeira.
- Derivação de um conjunto de recomendações para utilização pelos reguladores no desenvolvimento da política de cibersegurança.

2 MODELO DE PAGAMENTOS DIGITAIS E SERVIÇOS FINANCEIROS

Os serviços financeiros com um elemento significativo de inclusão financeira diferem dos serviços financeiros convencionais em vários aspetos chave, incluindo:

- **Segmento de clientes:** os serviços são oferecidos a segmentos da população até então não servidos ou mal servidos, que anteriormente realizavam a maioria das suas transações por meios informais.
- **Meio de transação:** trata-se tipicamente de tecnologia pesada, que envolve transações de autoatendimento ou assistidas por agentes realizadas por meio de um dispositivo digital.
- **Canal**: as transações são realizadas por meio de agentes ou diretamente por meio de um canal eletrónico, como um telemóvel.
- **Características dos segmentos de utilizadores:** muitos são clientes de baixa renda com pouca literacia digital ou financeira (embora se reconheça que seria uma simplificação grosseira caracterizar todos os clientes desta forma, é importante compreender que se aplica a uma proporção significativa).
- **Transações:** estas são tipicamente de baixo valor e baixo volume por cliente – os prestadores de serviços geralmente procuram compensar isto ao tentar alcançar um volume global elevado em todo o serviço.

Consequentemente, os riscos de cibersegurança que esses serviços enfrentam são um pouco diferentes, o que reflete as diferentes oportunidades de ataque e as limitadas oportunidades de defesa disponíveis. Além dos riscos diretamente abordados pelas principais frameworks de cibersegurança desenvolvidas e aplicadas com sucesso no mundo industrializado, existem classes muito específicas de risco que essas framework não abordam, o que dá o contexto em que foram desenvolvidas. Estes frameworks geralmente não incluem as considerações de inclusão financeira. Os riscos mencionados aqui são discutidos detalhadamente na Secção 3, juntamente com estratégias de mitigação.

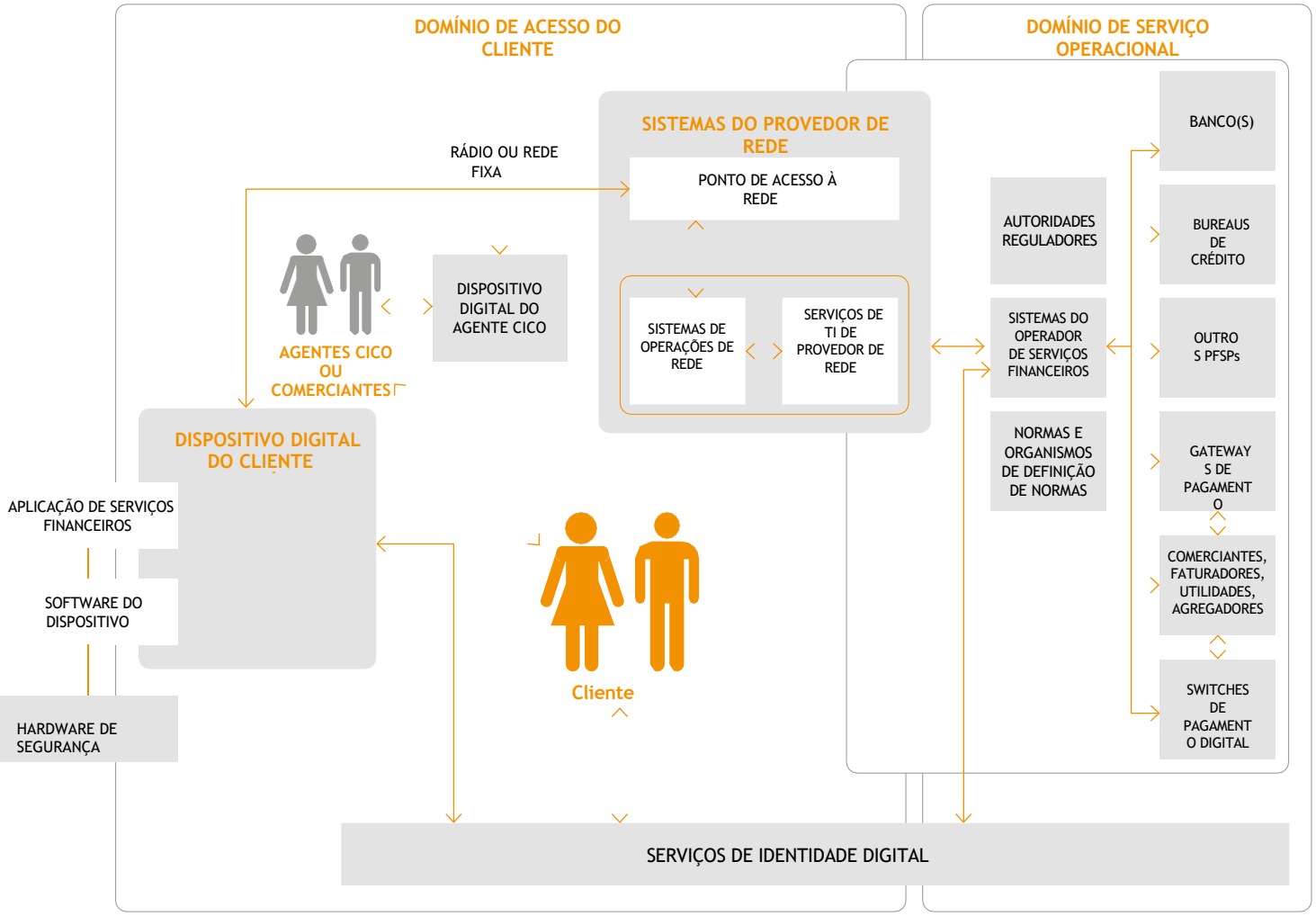
Para compreender estes riscos adicionais, é importante ter um modelo ou framework que sirva tanto como referência quanto como meio de classificação. Esta secção apresenta, portanto, um modelo de serviço abstrato para um serviço financeiro destinado parcial ou totalmente aos desfavorecidos. Este modelo destina-se a servir dois propósitos principais:

- Promover uma compreensão comum de como é um serviço – incluindo o "ecossistema de serviços" em que ele opera;
- Servir de ponto de referência para as próprias recomendações, ao contextualizar cada elemento.

O diagrama apresentado na Figura 1 apresenta o modelo de serviço utilizado na análise dos riscos de cibersegurança para inclusão financeira.

O modelo, apresentado sob a perspetiva do consumidor, ilustra a gama de intervenientes envolvidos na prestação de serviços e os variados meios de interconexão e interação entre eles. Foi ligeiramente abstraído para destacar os elementos e relações que interagem para fornecer um serviço financeiro com um elemento significativo de inclusão financeira. Em particular, pressupõe-se que a utilização por parte do consumidor de um dispositivo digital (como um telemóvel) ou de um serviço presencial seja uma característica de um serviço que apoia a inclusão financeira.

FIGURA 1: MODELO DE PAGAMENTOS DIGITAIS E SERVIÇOS FINANCEIROS



3 PRINCÍPIOS DE CIBERSEGURANÇA

3.1 INTRODUÇÃO

Este Guia fornece sete princípios fundamentais para a cibersegurança destinados especificamente a iniciativas de inclusão financeira.

- Dois princípios são para as autoridades reguladoras e de supervisão, a fim de melhorar os seus frameworks de supervisão, abordagens regulamentares e cooperação em matérias relacionadas com a cibersegurança dos serviços financeiros, com uma componente significativa destinada a dar resposta aos desafios da inclusão financeira.
- Os cinco princípios restantes estabelecem os requisitos a serem impostos aos prestadores de serviços e destinam-se a auxiliar as autoridades reguladoras na supervisão das atividades dos prestadores de serviços.

3.2 PRINCÍPIOS PARA REGULADORES, DECISORES POLÍTICOS E AUTORIDADES DE SUPERVISÃO

A cibersegurança não é um problema apenas para os prestadores de serviços. Dois princípios essenciais para garantir a segurança dos serviços e a proteção dos clientes são cumpridos pelas autoridades reguladoras e de supervisão.

PRINCÍPIO I: REGULAÇÃO E CONFORMIDADE

Estabelecer e manter os requisitos regulamentares que os prestadores de serviços devem cumprir; informar e auxiliar os prestadores de serviços na demonstração de sua conformidade com o ambiente regulatório; adaptar as regulamentações às mudanças nos ambientes; aplicação de abordagens baseadas em princípios e monitorização da segurança de infraestruturas públicas críticas.

PRINCÍPIO II: COOPERAÇÃO

Assegurar que as ações sejam tomadas em conjunto com os homólogos internacionais; cooperar com múltiplas agências nacionais ativas no domínio da segurança cibernética; partilhar informações sobre ameaças e incidentes e garantir que os PSFs tenham recursos humanos adequadamente qualificados para lidar com ameaças de cibersegurança.

3.3 PRINCÍPIOS PARA PRESTADORES DE SERVIÇOS

Estes princípios impõem requisitos aos prestadores de serviços quando prestam serviços financeiros com um elemento significativo de inclusão financeira e destinam-se a apoiar os reguladores na sua supervisão do cumprimento destes requisitos por parte dos prestadores de serviços:

PRINCÍPIO III: PROTEÇÃO AOS CLIENTES

Compreender as capacidades dos clientes em relação aos serviços financeiros; identificar os clientes; manter os seus dados privados e garantir a sua efetiva identificação durante a integração do cliente e nas transações.

PRINCÍPIO IV: PRESTAÇÃO DE SEGURO E SERVIÇOS

Compreender os canais de prestação de serviços e a infraestrutura que interagem entre os clientes dos PSFs, bem como garantir que a informação permaneça privada e que a integridade das transações seja mantida.

PRINCÍPIO V: GESTÃO DE RISCOS INTERNOS

Garantir que a integridade do serviço dos PSFs é preservada através de controlos e processos internos que proporcionem uma gestão de risco eficaz a nível empresarial para a prestação segura de serviços.

PRINCÍPIO VI: COMPREENDER SEUS PARCEIROS

Certificar-se de que os parceiros estão envolvidos através de processos apropriados sem aumentar significativamente os riscos para os clientes ou para o seu serviço.

PRINCÍPIO VII: O LONGO PRAZO

Garantir que o seu serviço mantenha a sua segurança à medida que surgem novas ameaças; informar as autoridades reguladoras tanto sobre os riscos existentes como sobre os seus planos para os enfrentar; realizar auditorias regularmente e garantir que todos os requisitos de relatórios sejam cumpridos etc.

3.4 REGULADORES

3.4.1 PRINCÍPIO 1: REGULAÇÃO E CONFORMIDADE

Estabelecer e manter os requisitos regulamentares em que os prestadores de serviços devem operar; informar e auxiliar os prestadores de serviços na demonstração de sua conformidade com o ambiente regulatório; adaptar as regulamentações às mudanças nos ambientes; aplicação de abordagens baseadas em princípios e monitorização da segurança das infraestruturas públicas críticas.

REFERÊNCIA	RECOMENDAÇÃO
R-1	Desenvolver ou adotar um framework de cibersegurança para orientar os PSFs quanto ao que se espera deles. Esse framework deverá ter em conta a adequação à dimensão da instituição regulamentada e aos riscos que apresenta para os clientes.
R-2	Considere as questões de responsabilidade que podem surgir se os padrões de segurança não forem seguidos pelos PSFs, especialmente se a não conformidade resultar em perda financeira. Questões a considerar incluem: > Comunicação obrigatória tanto à autoridade como aos clientes afetados > Requisitos para reembolsar perdas das contas dos clientes > Possíveis responsabilidades por perdas subsequentes dos clientes
R-3	Considere permitir padrões técnicos de segurança inferiores (incluindo, por exemplo, USSD) por meio do equilíbrio do risco mais elevado com uma responsabilidade mais rigorosa – consultar também Recomendação Referência C-10.
R-4	Desenvolver uma política para abordar os aspetos práticos da implementação dos procedimentos de supervisão, incluindo o desenvolvimento ou a adoção de um framework de avaliação da cibersegurança.
R-5	Dar especial ênfase à avaliação da qualidade, disponibilidade e instalações de monitorização contínua de transações pelos PSFs. Isto é especialmente no contexto do risco adicional incorrido pela utilização de USSD e SMS para serviços financeiros móveis.
R-6	Sempre que possível, nomeie um Chief Information Security Officer (CISO). Este indivíduo será responsável por desenvolver e implementar um programa de segurança da informação para proteger tanto os sistemas e dados internos, como os dados sensíveis fornecidos pelos PSF como parte das suas obrigações de relatório. O papel de CISO deve existir fora de quaisquer departamentos de TI ou Sistemas de Informação de Gestão. O benefício de tal função será resultante apenas da subordinação direta aos Diretores, evitando assim o risco de as preocupações com a cibersegurança serem filtradas pelos interesses de departamentos específicos. Essa prática recomendada do setor se aplica tanto às autoridades reguladoras quanto aos PSFs.
R -7	Os dados sensíveis fornecidos pelos PSF às autoridades de supervisão, incluindo dados sobre os seus clientes, devem estar sujeitos a muitas das mesmas medidas internas de cibersegurança que são exigidas aos PSFs. Para o efeito, as autoridades reguladoras/de supervisão devem ponderar a adoção de controlos técnicos internacionais de boas práticas em matéria de cibersegurança para utilização interna, tanto quando oferecem serviços digitais como quando são destinatários ou repositórios de dados confidenciais de entidades regulamentadas.
R -8	Estabelecer uma linha de base nacional para uma avaliação comum dos relatórios de preparação cibernética em todo o setor financeiro. Os PSFs são obrigados a realizar avaliações anuais do seu nível de preparação cibernética e fornecer os relatórios resultantes à autoridade de supervisão.
R -9	Desenvolver uma abordagem para fornecer uma avaliação adequada e padronizada da abordagem proposta por cada PSF para resolver quaisquer deficiências identificadas. As deficiências identificadas na avaliação de preparação cibernética de um PSF são geralmente abordadas num aditamento ao relatório de avaliação anual.
R-10	Revise os relatórios de transações suspeitas (RTSs) recebidos de PSFs individuais, por meio da comparação com os recebidos do restante do setor financeiro, e aja se eles diferirem significativamente no número esperado de relatórios ou no nível de detalhes fornecidos.
R-11	Visite regularmente os centros operacionais das PSFs para verificar se os processos documentados e os pontos de controlo estão a ser seguidos. Verifique também se a monitorização ativa de transações (incluindo a monitorização de AML) está em vigor, quando apropriado.
R -12	Desenvolver capacidade interna para cumprir os requisitos de supervisão estabelecidos neste documento.
R-13	Desenvolver programas de consciencialização em cibersegurança para entrega à Equipa de PSFs e autoridades regulatórias/supervisoras.
R -14	Incorporar cláusulas de aplicação efetiva em todas as diretrizes e frameworks nacionais de cibersegurança, de modo que a não conformidade de um PSF resulte em sanções de acordo com as regulamentações nacionais.
R-15	Tomar medidas para monitorizar a segurança de infraestruturas digitais críticas, incluindo sistemas de identidade digital, sistemas de pagamentos, switches financeiros etc. e agir para alertar os PSFs se um problema for identificado.

3.4.2 PRINCÍPIO II: COOPERAÇÃO

Assegurar que as ações sejam tomadas em conjunto com os homólogos internacionais; cooperar com múltiplas agências nacionais ativas no domínio da segurança cibernética; partilhar informações sobre ameaças e incidentes e garantir que os PSFs tenham recursos humanos adequadamente qualificados para lidar com ameaças de cibersegurança.

REFERÊNCIA	RECOMENDAÇÃO
O-1	Caso um PSF sofra uma falha na cibersegurança que conduza a uma violação de dados, ou no caso de a fraude ser comunicada às autoridades de supervisão, essas autoridades devem rever a ameaça cibernética associada e, se for caso disso, avisar outras entidades regulamentadas do ataque.
O-2	Deve-se considerar a criação de um organismo nacional de sensibilização e alerta cibernético; se o organismo de supervisão sentir que não há capacidade suficiente para isso, deve considerar identificar parceiros regionais ou internacionais para estabelecer tal serviço.
O-3	Configurar um Centro de Operações de Cibersegurança (CSOC) e uma Equipa de Resposta a Emergências Computacionais (CERT) em todo o setor.
O-4	Facilitar a cooperação entre o CSOC/CERT nacional e o CSOC/CERT regional/internacional que está em funcionamento.

3.5 PRESTADORES DE SERVIÇOS FINANCEIROS

Os requisitos estabelecidos na presente secção aplicam-se especificamente às atividades esperadas dos PSF com um elemento específico de inclusão financeira. Também visam ajudar as autoridades reguladoras na supervisão das atividades dos prestadores de serviços no cumprimento dos seus requisitos.

3.5.1 PRINCÍPIO III: O CLIENTE

Compreender as capacidades de atendimento financeiro dos clientes; identificá-los; manter seus dados privados e garantir que saiba quem eles são quando retornarem.

REFERÊNCIA	RECOMENDAÇÃO
C-1	**Capacidade de Serviços Financeiros** Os PSFs devem ter um programa de apoio e educação em vigor para clientes com literacia digital e/ou financeira limitada. O programa deve incluir aspetos relevantes dos riscos de cibersegurança e as medidas associadas que os clientes podem tomar para mitigá-los.
C-2	**Conheça o Seu Cliente (KYC) e Due Diligence Proporcionais e Baseados no Risco** É de vital importância que cada cliente de um PSF esteja sujeito a um processo robusto de identificação e verificação durante o registo, e que utilize apropriadamente inovações tecnológicas, como a análise da pegada digital de um cliente e serviços KYC partilhados ou baseados em utilidades. Isso não significa que cada cliente precise apresentar provas robustas da sua identidade. Em vez disso, uma abordagem proporcional ao KYC deve ser adotada: cada cliente deve apresentar qualquer documentação de identidade que tenha. Isto deve então ser sujeito a verificação, e o grau de acesso aos serviços financeiros deve ser construído com base no resultado desse processo, num modelo que segue as Recomendações da FATF. Desta forma, a um cliente potencial com uma identidade digital, emitida por um governo e sujeita a uma robusta autenticação biométrica, que também possa fornecer um passaporte e prova da sua morada, seria tipicamente oferecida a gama completa de serviços financeiros (sujeito a verificações adicionais caso a caso, como a determinação da solvabilidade). Em contraste, um cliente que só consiga fornecer um único documento de identidade em papel, como um cartão de eleitor, e não consiga fornecer documentação adicional, terá acesso apenas básico a uma conta transacional, com limites rigorosos de saldo e transação. Presume-se que haveria uma gradação de acesso entre estes dois extremos, possivelmente consistindo em três a cinco níveis. Em todos os casos, estas devem ser definidas de acordo com os requisitos estabelecidos na regulamentação nacional ou em acordo com as autoridades reguladoras (se isto não estiver definido de outra forma).
C-3	Os clientes devem ter a possibilidade de "atualizar" o nível de serviço a que podem aceder, ao fornecer documentação de identidade adicional ao PSF.
C-4	Deve também ser considerada a prestação de serviços a clientes que não conseguem apresentar qualquer tipo de documento de identidade, desde que um cliente existente do prestador de serviços financeiros apresente uma declaração da sua identidade. Naturalmente, isso deve estar sujeito a estritas condições: > Só deve ter lugar de acordo e sob a supervisão das autoridades competentes; > Se o cliente que atesta se tornar sujeito a investigação por qualquer motivo (identidade questionada; ligações a fraude, lavagem de dinheiro ou financiamento do terrorismo), então a conta do cliente atestado deve ser imediatamente suspensa.

REFERÊNCIA	RECOMENDAÇÃO
C-5	Uma vez tomada a decisão de conceder serviço a um cliente, deve ser criada uma "conta de registo de cliente". Esta será efetivamente uma identidade digital que é utilizada para aceder serviços. É diferente das contas de serviços financeiros e é utilizado para facilitar a gestão do relacionamento com o cliente, em vez da gestão dos serviços prestados ao cliente. O principal objetivo disso é garantir que todos os relacionamentos de um cliente com um PSF sejam adequadamente geridos. Isso ocorre para que uma abordagem focada no cliente seja adotada, em vez de uma abordagem focada no produto, o que apoia as atividades de AML e monitorização de transações do PSF. Esta conta de registo deve ser identificada por uma identidade do cliente, emitida ao cliente como um número de cliente ou outro token de identificação. A utilização do número de telemóvel de um cliente é aceitável, embora isso deva ser apoiado com procedimentos para gerir a mudança de números de telemóvel ao longo do tempo. Os controlos também devem ser implantados, uma vez que um número de telemóvel está sujeito a ataques, como o SIM Swap.
C-6	**Autenticação** Sempre que iniciar uma transação ou aceder dados privados (como sua conta ou detalhes da transação), os clientes devem ser obrigados a obter autenticação por meio das ferramentas fornecidas pelo PSF. A autenticação de fator único pode ser suficiente para transações de valor mais baixo ou visualização simples de contas, mas vários fatores (incluindo biometria) devem ser considerados para alterações de conta, início de transações maiores ou quando o volume geral em um período de tempo mais longo tiver atingido um limite definido.
C-7	**Privacidade e Proteção de Dados** Os dados do cliente, como os apresentados durante a integração e os gerados durante a vida útil do relacionamento com o PSF (incluindo dados de transação) devem ser adequadamente protegidos. Ele deve ser armazenado apenas de forma encriptada, e somente divulgado ao cliente ou a membros devidamente autorizados da equipa dos PSFs. As seleções de algoritmos criptográficos, comprimentos de chave, ferramentas de gestão de chaves etc., só devem ser feitas com base no conselho de especialistas em cibersegurança.
C-8	As transações presenciais (OTC) devem ser permitidas se o contexto específico de um país o exigir. No entanto, isso deve ser feito de forma cuidadosamente planeada, de modo que todas as partes envolvidas na transação sejam devidamente identificadas. Isso inclui o cliente iniciador, o agente iniciador, o agente recetor e o cliente recetor. Uma situação em que apenas os agentes estão ligados a uma transação, e os clientes permanecem anónimos, não é aceitável.
C-9	Se as limitações de literacia financeira significarem que um cliente ainda não está pronto para realizar as suas transações sozinho e beneficiaria de assistência (às vezes – embora nem sempre – a razão para a utilização de serviços presenciais), então devem ser-lhe oferecidos esses serviços; mas de forma conforme à recomendação anterior.
C-10	**Responsabilidade do Cliente** As responsabilidades dos clientes devem ser definidas tanto pelas capacidades dos clientes quanto pela viabilidade da sua influência sobre a fiabilidade e segurança do serviço. Durante as entrevistas realizadas, alguns stakeholders observaram que vários PSF têm um acordo com os clientes que os responsabiliza por quaisquer perdas no domínio de acesso do cliente (ver Figura 1). O resultado lamentável é que houve pouco ou nenhum investimento em melhor cibersegurança nesse domínio, mesmo que os clientes não tenham influência sobre, por exemplo, a segurança de uma rede móvel. Essa abordagem não é aceitável ou sustentável, pois afeta a confiança dos clientes no PSF e, de forma mais ampla, em todo o setor financeiro. Os clientes podem não estar cientes dessa responsabilidade, o que reforça a necessidade de ter mecanismos robustos de proteção ao cliente. Uma solução seria uma transferência de responsabilidade, de forma semelhante ao que se verifica na iniciativa PSD2 da União Europeia. Isto significaria que qualquer perda é automaticamente assumida como responsabilidade do PSF até prova em contrário e deve ser reembolsada ao cliente imediatamente. No entanto, se uma investigação subsequente revelar que a responsabilidade é, de facto, do cliente, o reembolso deve ser revertido. Em alguns casos, isto pode necessitar de uma reserva de fundos dedicada a reembolsos - mas em troca, os casos devem ser resolvidos rapidamente, idealmente dentro de três dias úteis.
C-11	**Alfabetização Digital** Cabe aos clientes serem vigilantes e garantir que outras pessoas não possam aceder às suas contas e realizar transações não autorizadas. Não devem, em circunstância alguma, divulgar o seu PIN ou palavra-passe a qualquer outra pessoa, não importa o quanto confiem nela. Se eles utilizam um smartphone, eles devem ser obrigados a instalar atualizações de segurança assim que estiverem disponíveis. Esta mensagem deve ser comunicada de forma clara - e enfatizada - ao cliente durante o registo.

3.5.2 PRINCÍPIO IV: PRESTAÇÃO DO SERVIÇO

Compreender os canais de prestação de serviços e a infraestrutura que fazem a interface entre os PSFs e seus clientes, bem como garantir que a informação permaneça privada e que a integridade das transações seja mantida.

REFERÊNCIA	RECOMENDAÇÃO
S-1	Os PSF devem fazer os melhores esforços para garantir que a segurança de ponta a ponta esteja implementada entre o cliente e os seus próprios sistemas internos. Os PSFs devem se referir a frameworks e padrões nacionais e internacionais de cibersegurança. Não se deve confiar na segurança de sistemas e redes externas. Estes raramente são concebidos e desenvolvidos tendo em mente a segurança de grau financeiro. Por exemplo, a segurança das redes de telefonia móvel foi concebida para: > Garantir que a receita da operadora móvel foi protegida contra acesso não autorizado; > Manter as conversas e os dados do telemóvel privados. O requisito de cibersegurança de um serviço financeiro é significativamente maior. Portanto, cabe ao PSF garantir a segurança, privacidade e integridade do seu serviço por si próprio.
S-2	Como foi destacado na Secção 2, a utilização do USSD para a prestação de serviços financeiros apresenta grandes vulnerabilidades de segurança: > Não há segurança desde o aparelho do cliente até os sistemas de backoffice de uma operadora móvel, o que pode permite que hackers espionem detalhes da conta e PINs e potencialmente levar à perda de fundos do cliente; > Um ciberatacante pode enviar uma sessão USSD para o cliente de uma maneira que pareça que o PSF está a entrar em contato com ele. Eles podem utilizar isso para pedir ao cliente que altere seu PIN, que pode ser capturado, o que pode levar ao sequestro de conta e perda de fundos. A mesma preocupação se aplica à utilização de SMS, que não deve ser utilizado para PINs únicos (OTPs) porque eles podem ser intercetados por ciberatacantes. A única exceção é a utilização de SIM Toolkit Apps que fazem sua própria encriptação de SMS, mas apenas quando essa encriptação foi revisada de forma independente. A recomendação não é que o USSD e o SMS sejam abandonados, embora isso seja preferível. No entanto, à luz das vulnerabilidades destacadas, a recomendação é, em primeiro lugar, que, onde o USSD/SMS é utilizado, a monitorização detalhada e ativa de transações seja implantada nos sistemas centrais do PSF para identificar e impedir transações fraudulentas. Em segundo lugar, deve ser implementada uma estratégia para gerir a migração para longe desses serviços expostos. Para as autoridades reguladoras, a recomendação é que, quando um serviço depende de USSD ou SMS não encriptado para entrega, os termos de serviço impostos aos clientes não devem imputar-lhes a responsabilidade por fraudes que ocorram no domínio de atendimento ao consumidor.
S-3	À medida que a penetração de smartphones aumenta, os PSFs devem considerar o fornecimento de uma aplicação adequadamente protegido para os clientes acederem seus serviços. O acesso ao aplicativo deve ser protegido com um PIN ou uma biometria (quando disponível), e os desenvolvedores da aplicação devem incluir defesas técnicas contra ciberataques. Por exemplo: > A aplicação deve ser encriptada para garantir que um invasor não possa fazer engenharia reversa da aplicação para extrair dados e chaves. > Quaisquer chaves criptográficas (por exemplo, para utilização em encriptação de ponta a ponta) devem ser quebradas e distribuídas (ocultas) ao redor do aplicativo e reconstruídas somente quando necessário. > A finalidade de todos os dados utilizados no aplicativo deve ser ofuscada, com a utilização de ferramentas de desenvolvimento adequadas. > O aplicação deve ser desenvolvido para operar na sandbox de um smartphone, quando disponível. Este é uma sandbox tecnológica para proteção criptográfica de serviços ao vivo e é diferente de uma sandbox regulatória. > Quando essa sandbox estiver disponível, a aplicação deve utilizar o Ambiente de Execução Segura (SEE) de um telemóvel. Este pode ser o SIM do telefone ou um SEE dedicado em um smartphone. > O PSF deve exigir que o cliente exija que o software do sistema operacional do smartphone esteja sempre atualizado; a aplicação não deve ser iniciado se o sistema operacional não oferecer o nível de segurança necessário. Além disso, a aplicação nunca deve ser iniciado se o telemóvel tiver sido 'jailbreak'. Os Controlos CIS-20 são um recurso útil nesta área.
S-4	Quando um PSF não é também um operador de rede móvel (ORM), esse PSF deve promover um bom relacionamento com todos os ORMs em seu país, a fim de restringir e monitorizar os swaps de SIM. As trocas de SIM devem ser desativadas para cartões que pertencem a indivíduos proeminentes ou aqueles que fazem parte do serviço do PSF (SIMs de agentes e funcionários). Isso ocorre a menos que a aprovação da alta administração do PSF seja obtida, já que os números de telemóvel desses indivíduos são frequentemente disponibilizados como parte de suas atividades normais e, portanto, são vulneráveis a ciberataques baseados em trocas de SIM. Várias trocas de SIM contra uma única conta em um curto período devem ser desativadas.
S-5	Nos casos em que exista um Centro Nacional de Operações de Cibersegurança (CSOC) e uma Equipa de Resposta a Emergências Informáticas (CERT), espera-se que o PSF contribua e participe nas suas atividades. Isso se soma ao requisito básico de conformidade com as normas nacionais e internacionais de cibersegurança emitidas pelas respetivas autoridades reguladoras.

3.5.3 PRINCÍPIO V: GESTÃO DE RISCOS INTERNOS

Garantir que a integridade do serviço de um PSF seja preservado por meio de controlos e processos internos, e que a equipa seja adequadamente gerida etc.

REFERÊNCIA	RECOMENDAÇÃO
I-1	A cibersegurança de um serviço financeiro pode ser prejudicada por funcionários mal-intencionados. Os PSFs devem, por conseguinte, realizar verificações de antecedentes específicas por país ao recrutar pessoal em posições sensíveis, incluindo: > Identificar adequadamente a equipa através dos mesmos processos de identificação e verificação utilizados ao integrar clientes; > Solicitar e consultar os registos policiais ou criminais apropriados para evitar o emprego de burlões conhecidos ou criminosos cibernéticos; > Os funcionários devem ser sujeitos a verificações de referências de crédito, onde estas estão disponíveis, para identificar aqueles com dívidas excessivas que possam, portanto, ser vulneráveis a subornos. Estas verificações de antecedentes devem aplicar-se a todo o pessoal em cargos superiores, incluindo pessoal sénior, qualquer pessoal de qualquer grau envolvido no acesso ou configuração da plataforma de SFD, ou atividades financeiras com parceiros bancários ou contas de clientes, e aqueles em funções voltadas para o cliente que estariam em posição de identificar contas para alvo de ciberatacantes. Além disso, essas verificações de antecedentes devem ser repetidas periodicamente.
I-2	Os empregadores devem aplicar uma redução robusta dos riscos no que diz respeito ao acesso aos sistemas informáticos para os seus trabalhadores críticos em posições sensíveis (definidos no ponto I-1). Esse acesso inclui regras de autorização, procedimentos de acesso, utilização restrita de dispositivos eletrónicos não autorizados em determinadas instalações de escritório, incluindo laptops pessoais, telemóveis, tablets etc.
I-3	É essencial que todas as interações do pessoal com a plataforma do PSF sejam registadas e que esses registos sejam autoritativos. Isto implica que todo o acesso do pessoal aos sistemas de IT está sujeito a autenticação forte, tal como autenticação de dois fatores; por exemplo, um nome de utilizador e uma palavra-passe, juntamente com um código QR que é digitalizado com a utilização do seu telemóvel. SMS para OTPs não é recomendado. O pessoal em posições sensíveis (que idealmente não devem ter os seus telemóveis consigo: ver I-2) devem ser fornecidos com um porta-chaves que gera códigos temporários, e a sua utilização deve ser obrigatório para todos os acessos. Por razões de auditabilidade, todas as atividades realizadas por todo o pessoal devem ser registadas, independentemente de essas atividades serem ou não bem-sucedidas. A trilha de auditoria resultante não deve ser editável, e o acesso a esses registos deve ser restrito. Esses registos devem ser auditados periodicamente.
I-4	Todas as funções operacionais e de gestão que a plataforma de serviço do prestador de serviços financeiros (PSF) fornece devem estar sujeitas a acesso baseado em funções, de modo que, por exemplo, se a sua função não envolver a movimentação de fundos ou o exame de contas de clientes, devem ser impedidos de aceder a essa funcionalidade.
I-5	O acesso baseado em função descrito no I-4 deve ser utilizado para implementar controlos de fabricante/verificador (às vezes chamados de controlos de "quatro olhos"), especialmente no que diz respeito à transferência de fundos e outras transações confidenciais. Este tipo de acesso permite que um membro da equipa "crie" ou crie os detalhes de uma transação de transferência de fundos, e outro "verifique/aprove" a transação. Nenhum indivíduo deve ser concedido ambos os papéis. Estes controlos devem ser reforçados pelo registo de logins e pela disponibilização de ferramentas de investigação e auditoria à gestão de topo e às autoridades externas.
I-6	Um elemento importante do planeamento de continuidade do negócio é a definição e operação de processos de negócio detalhados. Recomenda-se que isso seja realizado à medida que melhoram as operações de uma empresa e mitigam os problemas de erro da equipa, dependência excessiva de pessoal-chave e falta de compartilhamento de conhecimento entre a equipa. Deve ser adotado um sistema de gestão de processos de negócio (SGPN), que, quando implementado corretamente, pode gerir as operações diárias de um prestador de serviços financeiros de forma eficiente e reduzir a dependência de pessoal crítico.
I-7	O PSF deve identificar um conjunto de pontos de controlo, que podem ser incorporados aos processos de negócios, a fim de aprimorar a cibersegurança básica do serviço. Estes podem incluir: > A especificação de um valor de transação além do qual é necessária autorização adicional; > Uma pessoa específica cuja presença autenticada é necessária para realizar uma função; > Restrições sobre quando uma função específica pode ser realizada (por exemplo, durante o horário de expediente).
I-8	A reconciliação regular de transações entre contas de clientes e as contas bancárias do próprio PSF é uma atividade essencial, crucial para manter a integridade de um serviço financeiro. Neste contexto, a reconciliação tem duas funções principais: > Assegurar que todos os saldos dos clientes estão seguros. > Fornecer um indicador antecipado de possíveis fraudes perpetradas pela violação de controlos e controlos de cibersegurança para a criação de valor, seja interno ou externo.

REFERÊNCIA	RECOMENDAÇÃO
I-9	A encriptação é crucial para o funcionamento dos Serviços Financeiros Digitais (SFDs) e para a proteção e privacidade de dados. Ajuda a garantir a confidencialidade e integridade das comunicações entre: > Um PSF e seus clientes, fornecedores e outras partes externas; > O pessoal de um PSF e sistemas entre processos; > Os sistemas entre processos de um PSF (para evitar ataques de repetição). Todos os dados devem ser encriptados em trânsito e em repouso. Com relação aos dados em repouso, a intenção é que todos os dados do cliente, pessoais e de transação, sejam encriptados antes do armazenamento para que qualquer pessoa que possa obter acesso ao sistema não possa ver os dados. Isso sustenta o acesso baseado em função, para que apenas alguém que tenha se autenticado como portador das credenciais corretas possa ver os dados em claro. Todas as transações e atividades da equipa devem ser registadas para futuras auditorias ou investigações.
I-10	A segurança física é o primeiro passo para garantir a cibersegurança e limita a oportunidade para a subversão dos controlos cibernéticos. PSFs bem geridos se concentram igualmente em cibersegurança e segurança física. No mínimo, a segurança física envolve o seguinte: > Um, entrada estritamente controlada nas instalações de um PSF. > Garantir que outras entradas estejam seguras e que as saídas de incêndio tenham alarmes. > Garantir que todas as salas sejam protegidas com fechaduras biométricas e que exijam tanto "touch in" como "touch out" para evitar entrada não autorizada. Isso também significa garantir que o acesso a todas as salas seja restrito com base na função do trabalho (cargo). > Permissão de vigilância por vídeo e gravação 24 horas de todas as áreas. Isso é essencial para dissuadir e detetar crimes. Deve ser enfatizado que as câmaras não devem ficar voltadas para telas que possam exibir informações sensíveis. - No mínimo, essas gravações devem estar disponíveis por um período de um mês; no entanto, um ano é preferível. - Deve ser possível para investigadores autorizados descarregar e arquivar gravações para fins de investigação de fraude.
I-11	Recomenda-se que um PSF implemente funções ativas e automatizadas de monitorização e alerta de transações. Além da deteção e prevenção de fraudes, a monitorização ativa e automatizada de transações pode contribuir para as obrigações de conformidade de um PSF em relação ao combate à lavagem de dinheiro/combate ao financiamento do terrorismo (CLD/CFT).
I-12	Um responsável pela fraude deve ser nomeado. O papel é monitorizar transações, submeter relatórios de transações suspeitas às autoridades reguladoras e apoiar investigações adicionais em cooperação com essas autoridades.
I-13	O PSF deve implementar ferramentas modernas de investigação de transações com funcionalidade "follow the money", que podem ser utilizadas para investigação rápida e eficaz de potenciais crimes.
I-14	Organizações maiores com participação de mercado acima de 10% devem nomear um Diretor do Information Security Officer (CISO), responsável pelo desenvolvimento e implementação de um programa de segurança da informação.
I-15	Os PSFs devem fornecer a todo o pessoal operacional e de desenvolvimento habilidades em cibersegurança e formação de desenvolvimento.

3.5.4 PRINCÍPIO VI: COMPREENDER SEUS PARCEIROS

Garantir que os parceiros sejam engajados por meio de processos apropriados sem aumentar significativamente os riscos para os clientes ou para o serviço.

REFERÊNCIA	RECOMENDAÇÃO
P-1	Existem medidas adicionais de segurança física que se aplicam aos visitantes das instalações de um PSF, além daquelas que se aplicam aos membros da equipa: > Todos os visitantes devem ser identificados (com referência a um cartão de identidade ou similar) e registados. > Os visitantes não devem ser autorizados a levar nenhum equipamento eletrónico para áreas operacionais ou sensíveis. > Os visitantes podem ser autorizados a levar telemóveis e laptops apenas para áreas não operacionais. No entanto, os números de série dos laptops devem ser registados, e a equipa do PSF deve utilizar essas informações para verificar se os visitantes saem com o mesmo equipamento que trouxeram, para evitar a troca de laptops. > Os visitantes devem ser acompanhados em todos os momentos por um membro da equipa que é responsável por sua conduta. > Os funcionários nomeados devem estar sempre atentos à atividade dos visitantes. Em particular, os visitantes não devem ser autorizados a: - Vaguear pelo prédio sem acompanhamento; - Inserir unidades USB ou dispositivos similares em laptops da empresa, impressoras etc.
P-2	Deve ser desenvolvido e incorporado um processo na operação de um PSF para a integração de fornecedores e a subsequente gestão da relação. Os objetivos deste processo devem ser: > Capacitar a equipa de gestão do PSF a desenvolver a compreensão dos riscos que possam advir das atividades internas do fornecedor; > Compreender os relacionamentos do fornecedor com terceiros que, por exemplo, possam sujeitá-los à coerção para fornecer acesso impróprio às informações operacionais ou de clientes do PSF; > Identificar relacionamentos com funcionários-chave dentro do PSF, que possam ter o potencial de levar à colusão e fraude. Além de ser um componente vital da integração de fornecedores, esse processo de verificação também deve ser uma parte regular da due diligence anual, aplicada a todos os relacionamentos com fornecedores.
P-3	Ao estabelecer uma relação com um fornecedor, um PSF deve tomar medidas para garantir que há uma compreensão comum da divisão de responsabilidades e obrigações em caso de fraude.

3.5.5 PRINCÍPIO VII: O LONGO PRAZO

Garantir que um serviço de PSF mantém a sua segurança à medida que surgem novas ameaças; que as autoridades reguladoras sejam informadas dos riscos existentes e dos planos para os abordar; garantir que as auditorias sejam realizadas regularmente e que todos os requisitos de relatório sejam cumpridos etc.

REFERÊNCIA	RECOMENDAÇÃO
L-1	A administração e o conselho de administração de um PSF devem adotar e implementar as melhores práticas internacionais em cibersegurança. Utilizado de forma adequada, tal tornará mais simples a conformidade com os requisitos regulamentares e de supervisão nacionais emergentes.
L-2	A fim de ajudar no desenvolvimento contínuo da prontidão cibernética, cada PSF deve adotar uma ferramenta internacional de avaliação de cibersegurança de melhores práticas e integrar a utilização dessa ferramenta em seus principais processos de negócios, com o objetivo de aumentar o nível de prontidão para cibersegurança ao longo do tempo.
L-3	O Diretor/Gerente de TI de cada PSF deve adotar e implementar controlos técnicos internacionais de cibersegurança baseados em melhores práticas para reforçar a cibersegurança dos seus sistemas e serviços.
L-4	Com base em L-1 a L-3, um PSF deve desenvolver uma capacidade para identificar e lidar com novas ameaças de cibersegurança à medida que surgem.
L-5	Os PSFs devem avaliar o seu nível de prontidão cibernética, determinado através da utilização da Ferramenta de Avaliação de Cibersegurança do FFIEC. Este processo de revisão deve ser realizado pelo menos anualmente, e as autoridades reguladoras e de supervisão devem ser informadas dos resultados.
L-6	Quando o nível de preparação cibernética de um PSF não atinge os padrões esperados, o PSF deve informar as autoridades reguladoras e de supervisão dos seus planos para resolver a lacuna, com referência particular ao PCS do FSSCC.
L-7	Qualquer falha na cibersegurança que conduza a uma violação de dados ou fraude deve ser comunicada imediatamente às autoridades competentes.

3.6 RESUMO DOS RISCOS

A tabela seguinte lista os principais intervenientes; descreve o seu papel na prestação de serviços financeiros; destaca os principais riscos a que estão expostos e define os impactos ou implicações de alto nível desses riscos se se concretizarem.

TABELA 1: PAGAMENTOS DIGITAIS E SERVIÇOS FINANCEIROS: INTERVENIENTES, PAPÉIS, RISCOS E IMPACTOS

ATOR	DESCRIÇÃO	PRINCIPAIS RISCOS	IMPACTOS
Cliente	O cliente pode ou não utilizar um dispositivo digital, como um telemóvel, para aceder os serviços.	> Baixa literacia financeira, digital e/ou cibernética > Engenharia social, a possibilitar fraudes contra o cliente > Erros	> Perda de fundos > Perda de dados pessoais
Dispositivo digital do cliente	O cliente pode utilizar um dispositivo para aceder o serviço ou utilizar um serviço OTC.	> Hacking > Escutas	Perda dos fundos do cliente
Aplicação de serviços financeiros	> Uma aplicação que o cliente pode utilizar em suas interações com o serviço, incluindo transações. > Pode ser fornecido pelo PSF ou por uma FinTech.	> Hacking > Intercetação/Escutas	> Perda de fundos > Perda de dados pessoais
Comerciante	Quer vender para o cliente e está disposto a aceitar pagamento via dispositivo digital.	> Baixa literacia digital > Formação inadequada	Disponibilidade de serviço reduzida; confiança reduzida.
Dispositivo digital do comerciante	O dispositivo digital do comerciante pode ser um telemóvel.	> Hacking > Escutas	Perda dos fundos do cliente ou do comerciante
Agente	> Presta serviços ao cliente. Esses serviços podem incluir o registo de clientes, serviços de depósito/levantamento (CICO) ou uma gama completa de serviços financeiros através de um modelo presencial. > Em algumas circunstâncias, um comerciante também pode assumir o papel de agente.	> Baixa literacia digital > Formação inadequada > Pessoal não fiável	> Disponibilidade e confiabilidade reduzidas do serviço > Fraude contra o cliente > Fraude contra o agente (por parte do pessoal)
Dispositivo digital do agente	Utilizado para prestar serviços a clientes e para gerir a prestação de serviços. Pode ser um telemóvel.	> Hacking > Escutas	Disponibilidade de serviço reduzida; confiança reduzida
Serviço de identidade digital	Utilizado para estabelecer a identidade do cliente durante a integração. Em alguns países, esse serviço também oferece serviços de autenticação para utilização durante transações financeiras, mas, geralmente, a função de autenticação é executada pelo PSF.	> Registo fraco > Autenticação fraca durante a integração > Consequente ligação a registos incorretos nos serviços de informações de crédito, o que facilita a fraude.	> Identificação de cliente pouco fiável > Fraude (ou outros crimes) não rastreáveis > Empréstimos inadequados por parte do PSF
Regulatório autoridades	Definir o ambiente regulatório e de supervisão ambiente nos quais os serviços podem ser oferecida, e identificar o pessoal que deve garantir que essas expectativas são cumpridos.	Falta de familiaridade com riscos técnicos (fintech, serviços financeiros digitais, redes móveis)	> Distribuição inadequada de responsabilidade > Diminuição do cliente proteção > Perda de confiança nos serviços
Padrões & configuração padrão organismos	Definir como os diferentes parceiros na prestação de serviços podem interoperar e estabelecer as expectativas colocadas na qualidade desse serviço.	Normas inadequadas que resulta em insegurança, inadequado ou não fiável serviços	> Confiabilidade reduzida > Perda de confiança nos serviços

Rede de comunicações	Pode ser um telemóvel ou rede Wi-Fi ou uma configuração semelhante.	> Escutas > Intercetação > Redireccionamento > Falsificação > Phishing	> Perda de fundos de clientes, agentes ou comerciantes > Sequestro de conta de cliente > Perda de dados de clientes ou comerciantes
Sistemas de um operador de rede	Estes são compostos por: > Estações base da rede operacional, localizadas em todo o país, que fornecem acesso local a uma espinha dorsal que interliga toda a rede; > Um centro de operações de rede central, que é composto por sistemas de operações de rede (estes prestam o serviço de comunicações) e os sistemas internos de TI do operador de rede, que administram os sistemas operacionais e prestam suporte administrativo.	> Phishing > Falsificação > Escutas > Intercetação	> Perda de fundos de clientes, agentes ou comerciantes > Sequestro de conta de cliente, agente ou comerciante > Perda de dados de clientes, agentes ou comerciantes
Os sistemas do PSF	Utilizado para prestar serviços financeiros a clientes, potencialmente incluindo os desassistidos.	> Controlos internos inadequados > Intervenientes mal-intencionados internos > Falta de planejamento de continuidade de negócios > Ferramentas deficientes de investigação de fraude	> Violações de dados; perda de dados de serviço, tanto financeiros como não financeiros > Serviço não fiável > Perda de reputação > Incapacidade de combater o crime financeiro
Bancos	> Mantém os fundos dos clientes. > Note-se que o banco e o PSF (Prestador de Serviços Financeiros) podem ser a mesma organização, embora não seja incomum que sejam entidades separadas.	> Falha em realizar uma reconciliação adequada, que resulta em risco adicional de fraude. > Concentração de fundos; potencial falência bancária que resulta na perda dos fundos dos clientes. > Intervenientes mal-intencionados internos	Falência sistémica
Outros prestadores de serviços externos	Apoiar o PSF na prestação de seus serviços. Por exemplo, isto pode incluir parceiros técnicos, como serviços de servidores/hospedagem, ou parceiros logísticos responsáveis pela gestão de redes de agentes.	> Interrupção de serviços > Hacking > Falsificação	Perda de reputação e, portanto, de confiança
BUREAUS DE CRÉDITO	Apoiar o PSF na prestação de seus serviços	Erros de registo de crédito	Risco financeiro para o PSF decorrente de empréstimos inadequados

3.7 DE NOTA ESPECIAL: USSD, SMS E RISCO CIBERNÉTICO

O USSD é amplamente utilizado na prestação de serviços financeiros aos desfavorecidos, e reconhece-se que isto é frequentemente necessário por uma série de razões que estão além do âmbito deste documento. No entanto, o USSD tem grandes vulnerabilidades de segurança:

- Não há segurança desde o aparelho do cliente até os sistemas de backoffice de uma operadora móvel, o que pode permite que hackers espionem detalhes da conta e PINs e potencialmente levar à perda de fundos do cliente;
- Um ciberatacante pode enviar uma sessão USSD para o cliente de uma maneira que pareça que o PSF está a entrar em contato com ele. Eles podem utilizar isso para pedir ao cliente que altere seu PIN, que pode ser capturado, o que pode levar ao sequestro de conta e perda de fundos.

A mesma preocupação se aplica à utilização de SMS, que não deve ser utilizado para PINs únicos (OTPs) porque eles podem ser intercetados por ciberatacantes; a única exceção é a utilização de SIM Toolkit Apps que fazem sua própria encriptação de SMS.

Até que a tecnologia para proteger totalmente os dados privados esteja disponível para clientes e PSFs, e as transações se tornem mais acessíveis, deve haver uma monitorização cuidadosa e sustentada das transações pelos PSFs. Com isso, os PSFs devem priorizar a identificação de anomalias e a intervenção adequada. As abordagens para mitigar esses riscos estão incluídas na Secção 3.5.2 deste documento.

4 ANTECEDENTES: FRAMEORKS EXISTENTES

4.1 INTRODUÇÃO

Os reguladores e supervisores do setor financeiro estarão bem cientes de que já existe uma vasta gama de framework de cibersegurança: alguns generalizados, outros destinados a proteger a infraestrutura crítica de uma nação, algumas formalizadas em padrões nacionais ou internacionais, e outras específicas para um determinado setor da economia, incluindo o setor financeiro.

Não é objetivo deste documento oferecer uma alternativa a esses frameworks. Em vez disso, como foi destacado na Secção 1.2.1, este Guia pretende complementar os frameworks, ao destacar e enfatizar os riscos que surgem da adoção de práticas e tecnologias que se tornaram comuns quando um serviço está focado nas prioridades da inclusão financeira.

Na busca deste objetivo, é importante destacar o panorama dos frameworks de cibersegurança em relação aos quais este documento deve ser visto. Com base em entrevistas com uma vasta gama de stakeholders, é apresentada nesta secção uma visão consensual do amplo conjunto de frameworks supranacionais de cibersegurança relevantes para as autoridades reguladoras e os PSFs.

Além disso, as autoridades reguladoras de vários países tomaram a iniciativa no desenvolvimento de frameworks nacionais de cibersegurança que se relacionam com todo o setor financeiro no seu país, sem ênfase específica na inclusão financeira. Alguns destes estão também resumidos nesta secção.

4.2 FRAMEWORKS SUPRANACIONAIS

No que diz respeito aos frameworks supranacionais de cibersegurança, os stakeholders salientaram repetidamente a importância e a relevância dos frameworks nas subsecções seguintes.

4.2.1 NIST

O Instituto Nacional de Padrões e Tecnologia (NIST) dos EUA publicou seu primeiro framework de cibersegurança em 2014. Este é um framework influente, que sustenta muitas dos outros frameworks de cibersegurança publicadas por outros organismos ao redor do mundo. O NIST publicou[1] a versão atualizada (1.1) de seu Framework for Improving Critical Infrastructure Cybersecurity em 16 de abril de 2018.

Desde a publicação da versão 1.0 em fevereiro de 2014, o NIST Framework tornou-se a posição inicial padrão para muitas organizações que desejam abordar questões de cibersegurança. Não obstante o seu estatuto fundamental e influente, o NIST Framework é muito geral; destina-se a melhorar a cibersegurança das infraestruturas críticas em todos os setores de uma economia e não pode ser utilizado diretamente pelos PSFs sem ser mais específico. As secções a seguir documentam algumas abordagens a esse respeito.

4.2.2 FFIEC

O Federal Financial Institutions Examination Council (FFIEC) baseou-se no framework de cibersegurança do NIST e desenvolveu uma ferramenta de avaliação de cibersegurança, especificamente voltada para o setor financeiro, permitindo que as instituições para avaliar sua própria prontidão para cibersegurança. A ferramenta foi publicada[2] em maio de 2017, em resposta ao aumento do volume e sofisticação das ameaças cibernéticas. O desenvolvimento da ferramenta foi moldado pelo framework de cibersegurança do NIST.

O objetivo da ferramenta é ajudar as instituições financeiras a identificar seus riscos e determinar sua preparação para a cibersegurança. Além disso, está estruturada para fornecer a essas instituições um processo repetível e padronizado para medir o desenvolvimento da sua preparação em cibersegurança ao longo do tempo.

A abordagem do FFIEC é amplamente admirada e adotada, e tem sido influente em uma série de iniciativas, incluindo a CROE do Banco Central Europeu, que é resumido mais adiante nesta secção.

4.2.3 CPMI-IOSCO

O Comité de Pagamentos e Infraestruturas de Mercado (CPMI) do Banco de Pagamentos Internacionais (BIS), em colaboração com o Conselho da Organização Internacional das Comissões de Valores Mobiliários (IOSCO), desenvolveu o documento[3] para "Orientações sobre resiliência cibernética para infraestruturas dos mercados financeiros" (Orientações Cibernéticas) em junho de 2016. A Orientação aplica-se a uma Infraestrutura do Mercado Financeiro (FMI) nacional completa, definida como "instituições de importância crítica responsáveis por fornecer compensação, liquidação e registo de transações monetárias e outras transações financeiras".

As orientações baseiam-se em princípios e não no estabelecimento de normas específicas, em reconhecimento da natureza dinâmica da cibersegurança e das ameaças que representam para os sistemas e serviços. Um aspeto importante a enfatizar é que se destina a complementar - e não a substituir - diretrizes de cibersegurança centradas em TI. Por outro lado, enfatiza que a cibersegurança é mais do que apenas TI.

1 https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

2 https://www.ffiec.gov/cyberassessmenttool.htm

3 https://www.bis.org/cpmi/publ/d146.htm

Assim, sugere que uma organização necessita tanto de um framework baseado em princípios quanto de um framework de cibersegurança de TI, a trabalhar em conjunto para garantir a segurança de uma instituição financeira contra ameaças cibernéticas.

4.2.4 CROE do BCE

O Banco Central Europeu (BCE) publicou[4] as suas "Expectativas de supervisão de resiliência cibernética para infraestruturas de mercados financeiros" (CROE) em dezembro de 2018. No desenvolvimento da CROE, o BCE considerou uma série de documentos e frameworks de orientação internacionais – nomeadamente CPMI-IOSCO, NIST e FFIEC. O objetivo da CROE é ajudar as autoridades de supervisão/monitorização na sua tarefa de rever a conformidade com as orientações do CPMI-IOSCO como parte da sua função de supervisão; em essência, é semelhante a um framework de avaliação.

A CROE do BCE é um documento importante que fornece uma ponte extremamente útil dos requisitos estabelecidos no CPMI-IOSOC, NIST e em outros lugares, para os processos que as instituições financeiras devem ter em vigor para alcançar a conformidade. Isso é feito de uma maneira que é relevante para o estado de evolução da instituição e o ambiente em que opera.

No entanto, ele não foi concebido como ou pretende ser um framework formal de cibersegurança. Isso reflete o seu papel primordial como uma ferramenta para uso das autoridades de supervisão/fiscalização. A CROE auxilia as autoridades na avaliação dos frameworks de cibersegurança utilizadas pelas organizações cuja supervisão elas são responsáveis. Essencialmente, ajuda a desenvolver a capacidade das autoridades para avaliar a cibersegurança das instituições que supervisionam, um elemento essencial do puzzle da cibersegurança.

4.2.5 PERFIL DE CIBERSEGURANÇA DO FSSCC

O Conselho de Coordenação do Setor de Serviços Financeiros dos EUA (FSSCC) foi estabelecido em 2002 por representantes do setor financeiro nos Estados Unidos. Trabalha em colaboração com agências governamentais dos EUA para proteger a infraestrutura crítica do setor financeiro dos EUA contra incidentes cibernéticos e físicos. O FSSCC lançou a versão 1[5] de seu Perfil de Cibersegurança (PCS) em 25 de outubro de 2018. O framework é baseado fortemente no Framework NIST e Orientações do CPMI-IOSCO. Perguntas de avaliação são baseados em orientações e framework de supervisão relevantes e mapeamentos para controlos ISO/IEC 27001/2.

O desenvolvimento do PCS do FSSCC surgiu, pelo menos em parte, como uma resposta à abordagem fragmentada de regulamentos e frameworks existentes. A maioria deles é derivada das Funções, Categorias e Subcategorias do NIST Framework, mas eles fornecem apenas cobertura parcial, ou adotam uma abordagem tão arbitrária que a utilidade é comprometida.

O FSSCC se propôs a evitar isso ao adotar uma direção abrangente e pan-setorial. Apesar disso, deve ser lembrado que a sua origem está no setor financeiro dos Estados Unidos, que pode ter uma capacidade diferente das instituições financeiras (especialmente as menores) e das agências de supervisão em economias emergentes.

4.2.6 CENTRO DE SEGURANÇA NA INTERNET – OS CONTROLOS CIS 20

Refletindo a recomendação do CPMI-IOSCO de que uma organização precisa de um framework baseado em princípios e um framework de cibersegurança de TI, vários stakeholders destacaram o valor do "CIS 20" como um exemplo líder deste último.

O Center for Internet Security (CIS) é uma entidade sem fins lucrativos sediada nos EUA. Nas suas palavras, "aproveita o poder de uma comunidade global de TI para proteger organizações privadas e públicas contra ameaças cibernéticas". Isto é de particular interesse devido à sua abordagem "de baixo para cima" à cibersegurança. Em vez de um conjunto dos princípios mandatados pelos reguladores, autoridades de supervisão ou consórcios dos principais bancos, a abordagem do CIS baseia-se na experiência proporcionada por quem lida com a cibersegurança de forma contínua e ativa. É, portanto, um complemento útil para outras abordagens.

De particular relevância para este Guia é o que ficou conhecido como "Controlos CIS 20". Trata-se de um conjunto de 20 controlos e diretrizes de cibersegurança que, quando tomadas em conjunto, atendem às necessidades de cibersegurança da maioria das organizações, incluindo as do setor financeiro. A versão atual no momento da escrita é a 7.1[6], lançada em 1 de abril de 2019. Uma publicação separada que documenta o alinhamento com o Framework de Cibersegurança do NIST está disponível no CIS, embora não tenha sido revisada na preparação deste Guia.

4 https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

5 https://www.ffiec.gov/cyberassessmenttool.htm

6 https://www.cisecurity.org/controls/

4.3 FRAMEWORKS NACIONAIS

4.3.1 INTRODUÇÃO

Ao considerar os frameworks nacionais de cibersegurança liderados pelas autoridades reguladoras, as entrevistas com os stakeholders identificaram três, em particular, como refletindo uma crescente sofisticação nas respostas das agências nacionais às crescentes preocupações em matéria de cibersegurança no setor financeiro:

- a "Ferramenta de Avaliação de Maturidade em Cibersegurança" da Arménia;
- a "Diretiva de Cibersegurança e Segurança da Informação" de Gana;
- A "Framework de Cibersegurança Baseada em Risco" da Nigéria.

Coincidentemente, todos os três foram publicados em 2018, o que reflete tanto a crescente urgência sentida pelas autoridades regulatórias em economias emergentes quanto sua disposição de se envolver ativamente com o setor financeiro para abordar as questões.

A natureza destes frameworks varia consideravelmente, como já foi visto com os frameworks supranacionais. Isso está relacionado, em parte, às prioridades de cada autoridade nacional individual. Os frameworks nigeriano e ganês fornecem uma especificação clara do que é esperado das instituições financeiras (e, nisso, são semelhantes ao PCS do FSSCC), enquanto o framework arménio se foca em como – através de atividades individuais detalhadas – uma instituição financeira pode alcançar o grau necessário de cibersegurança (semelhante ao framework do FFIEC).

4.3.2 ARMÉNIA

Durante o período de 2007 a 2010, com o objetivo de melhorar a governança, os processos e os procedimentos de TI e de segurança da informação, o Banco Central da Arménia (CBA) adotou a norma ISO 27001 para sistemas de gestão de segurança da informação, o que levou à certificação em 2012. Durante esse período, a CBA definiu regulamentos de cibersegurança para instituições financeiras regulamentadas, com a utilização de um conjunto simplificado de requisitos com base na ISO 27001. Em 2013, o CBA estendeu esta exigência e determinou que todas as instituições financeiras fossem certificadas pela norma ISO 27001 até 2015, com a certificação a ser realizada por um organismo de certificação internacionalmente reconhecido.

Mais recentemente, a área de Auditoria Interna da CBA desenvolveu uma ferramenta de autoavaliação de cibersegurança, inicialmente para utilização interna e, posteriormente, para utilização por instituições financeiras regulamentadas. Esta ferramenta destina-se a ajudá-los (e às autoridades de supervisão) a desenvolver uma compreensão do seu perfil de risco inerente e maturidade em cibersegurança.

Trata-se de um instrumento valioso que, através da automatização do framework do FFIEC, oferece um passo significativo na usabilidade desse framework. A sua utilização pelas instituições financeiras deve, portanto, ser promovida. No entanto, como poderia ser utilizado pelas autoridades de supervisão/fiscalização não foi determinado.

4.3.3 GANA

Em outubro de 2018, o Banco de Gana publicou[7] a "Diretiva de Cibersegurança e Segurança da Informação", que é destinada ao setor de serviços financeiros em Gana, e que:

> "…fornece um framework para estabelecer protocolos e procedimentos de Cibersegurança e da Informação para; cenários rotineiros e de emergência, delegação de responsabilidades, comunicação e cooperação inter e intraempresa, coordenação com as autoridades governamentais, estabelecimento de mecanismos de relatório, medidas de segurança física para Datacenters e Salas de Controlo de TI, e garantia da segurança de dados e redes."

No que diz respeito às regulamentações e normas internacionais, o documento faz particular referência ao ISO27001[8] (segurança da informação), ISO27032[9] (diretrizes para a cibersegurança), PCI-DSS (segurança das transações com cartões) e ao framework e diretrizes de cibersegurança[10] publicados pelo NIST com sede nos EUA, cuja experiência nesta área é amplamente reconhecida.

A Diretiva divide-se em várias partes, o que estabelece requisitos para os sistemas e serviços e define as responsabilidades dos principais intervenientes. Estes requisitos cobrem uma ampla gama e cada um contém uma grande quantidade de conselhos altamente relevantes e úteis.

A Diretiva representa um passo em frente significativo para garantir a cibersegurança dos PSFs no Gana, com consideração tanto às abordagens recomendadas quanto à amplitude de sua visão.

4.3.4 NIGÉRIA

Ao reconhecer o rápido crescimento das transações em todo o setor financeiro da Nigéria (incluindo o emergente setor de fintech) e a crescente prevalência de ciberataques a instituições financeiras, o Banco Central da Nigéria (CBN) emitiu seu Framework de Cibersegurança Baseado em Risco[11], aplicável a todos os bancos que aceitam depósitos e prestadores de serviços de pagamento, em 10 de outubro de 2018, e a data para a conformidade total foi definida para 1º de janeiro, de 2019. Isto seguiu-se a um projeto anterior emitido em Junho de 2018, que foi revisto após consulta à indústria.

---

7 https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

8 Uma especificação para um sistema de gestão da segurança da informação (ISMS). Um ISMS é um framework de políticas e procedimentos que inclui todos os controlos legais, físicos e técnicos envolvidos nos processos de gestão de riscos de informação de uma organização.

9 Antecedentes: A ISO 27032 não é uma norma que se pode certificar; esta é uma das diferenças mais importantes em relação à ISO 27001, que visa a certificação de um ISMS. O principal objetivo da ISO 27032 é fornecer um guia para a cibersegurança por meio de recomendações específicas. Assim, o foco da ISO 27001 é uma organização e o seu ISMS, enquanto a ISO 27032 se foca no ciberespaço e é um framework para colaboração.

10 https://www.nist.gov/cyberframework

11 https://www.cbn.gov.ng/out/2018/bsd/risk%20based%20cybersecurity%20framework%20final.pdf

O framework da CBN adota uma abordagem diferente daquela instituída por Gana: a de estabelecer diretrizes amplas, com referência a especialistas/autoridades internacionais, como NIST e PCI-DSS, para orientação detalhada.

Alguns aspetos importantes do CBN Framework são:

- O Diretor de Segurança da Informação (CISO) de uma instituição financeira deve relatar diretamente ao CEO. Em nenhuma circunstância o CISO deve relatar ao Chefe de TI. Embora seja uma prática recomendada no setor, a importância deste aspeto não pode ser subestimada.
- Como parte de uma autoavaliação de resiliência de cibersegurança, o framework inclui um requisito para que as instituições determinem seu perfil de cibersegurança atual e o estado desejado/alvo, juntamente com um roteiro detalhado para atingir a meta dentro de um prazo estipulado.
- São definidos requisitos mínimos para estabelecer e desenvolver a resiliência operacional de cibersegurança, incluindo a necessidade de compreender os ambientes operacionais, tecnológicos e de negócios de uma instituição;
  melhorar continuamente a resiliência de cibersegurança e desenvolver uma capacidade de inteligência contra ameaças cibernéticas.
- Existe um requisito para todas as instituições relatarem todos os ciberataques ao CBN, sejam eles bem-sucedidos ou não, dentro de 24 horas após a sua ocorrência. Não está claro qual é o alcance disso. Presumivelmente, não inclui os ataques gerais de "sondagem" que
  ocorrem continuamente na Internet, à medida que os atacantes investigam os sistemas para detetar portas eletrónicas óbvias que foram deixadas abertas [12]. Seria útil obter alguma clareza sobre o limiar antes de um relatório ser exigido ou gerado.

O CBN Framework, como seria de esperar, é um recurso importante e valioso, que estabelece princípios claros e fornece uma grande quantidade de orientações aos PSFs sobre como eles podem garantir a conformidade.

12 Qualquer dispositivo conectado à Internet pode esperar ver sua conexão com a Internet investigada muitas vezes em um dia, contando com uma firewall para protegê-lo.

GLOSSÁRIO

PRAZO	DESCRIÇÃO
AFI	Alliance for Financial Inclusion
AML	Contra Lavagem de Dinheiro
API	Interface de Programação de Aplicações
BIS	Banco de Compensações Internacionais
BoG	Banco de Gana
SGPN	Sistema de Gestão de Processos de Negócios
CA	Autoridade Competente
CAF	Framework de Avaliação Cibernética
CBA	Banco Central da Arménia
CBN	Banco Central da Nigéria
CERT	Equipa de Resposta a Emergências Computacionais
CFT	Combate ao financiamento do terrorismo
CICO	Entrada de dinheiro, Cash Out
CII	Infraestrutura Crítica de Informações
CEI	Centro de Segurança na Internet
CISO	Diretor de Riscos de Segurança da Informação
CNI	Infraestrutura Nacional Crítica
CPMI	Comité de Pagamentos e Infraestruturas de Mercado
CROE	Expectativas de Supervisão da Resiliência Cibernética
CSA	Agência de Cibersegurança
CSIRT	Equipa de Resposta a Incidentes de Segurança Informática
CSOC	Centro de Operações de Cibersegurança
PCS	Perfil de Cibersegurança
SFDs	Serviços Financeiros Digitais
DFS WG	Grupo de Trabalho de Serviços Financeiros Digitais
DGSSI	Direção Geral de Sistemas de Segurança de Informação
ENISA	Agência da UE para a Segurança das Redes e da Informação
UE	União Europeia
FATF	Força-Tarefa de Ação Financeira
FFIEC	Conselho Federal de Exame de Instituições Financeiras
FI	Inclusão Financeira ou Instituição Financeira, a depender do contexto
Fintech	Produtos de Tecnologia Financeira
Fintech	Empresa ou Prestador De Serviços de Tecnologia Financeira
FMI	Princípios para Infraestruturas do Mercado Financeiro
PSF	Prestador e Serviços Financeiros

PRAZO	DESCRIÇÃO
FSSCC	Conselho Coordenador do Setor de Serviços Financeiros
IGP	Indicador de Boas Práticas
IOSCO	Organização Internacional das Comissões de Valores Mobiliários
ISMS	Sistema de Gestão de Segurança da Informação
AMS	Autoridade Monetária de Singapura
IMF	Instituição de Microfinanças
ORM	Operadora de Rede Móvel
NCSC	Centro Nacional de Cibersegurança
NCSS	Estratégia Nacional de Cibersegurança
NIS	Redes e Sistemas de Informação
OES	Operadoras de Serviços Essenciais
OTC	Presencialmente
OTP	PIN único
PEP	Pessoa Politicamente Exposta
PIN	Número de Identificação Pessoal
PFMI	Princípios para Infraestruturas do Mercado Financeiro
RegTech	Tecnologia Regulatória
RFP	Solicitação de Proposta
SACCO	Organização Cooperativa de Poupança e Crédito
SEE	Ambiente de Execução Seguro
PME	Empresa de Pequeno ou Médio Porte
SMS	Serviço de Mensagens Curtas
SOC	Centro de Operações de Cibersegurança
RTS	Relatório de Transações Suspeitas
SupTech	Tecnologia de Supervisão
TRM	Gestão de Riscos Tecnológicos
USSD	Dados de Serviços Suplementares Não Estruturados

ANEXO A
ENTREVISTAS COM OS STAKEHOLDERS

Os seguintes stakeholders foram entrevistados durante a preparação deste documento.

NOME	TÍTULO	ORGANIZAÇÃO	FUNÇÃO
Komitas Stepanyan	Vice-Chefe de Auditoria Interna	Banco Central da Arménia	Autoridade Reguladora
Daniel Klu, CISO	Diretor de Riscos de Segurança da Informação	Banco de Gana	Autoridade Reguladora
Hakima El Alami	Diretor Adjunto responsável pela Supervisão de Sistemas e Meios de Pagamento e Inclusão Financeira	Bank Al-Maghrib, Marrocos	Autoridade Reguladora
Fadwa Jouali	Chefe de Fintech e Desenvolvimento de Pagamentos	Bank Al-Maghrib, Marrocos	Autoridade Reguladora
Mustapha Hadadi	Departamento de Organização e Sistema de Informação	Bank Al-Maghrib, Marrocos	Autoridade Reguladora
Stephen Mathew Ambore	Chefe de Serviços Financeiros Digitais,	Banco Central da Nigéria	Autoridade Reguladora
Candy Ngula	Diretor Adjunto	Banco da Namíbia	Autoridade Reguladora
Thomas Lammer	Especialista Principal em Infraestrutura de Mercado, Divisão de Supervisão	Banco Central Europeu	Autoridade Reguladora
Klaus Löber	Chefe de Divisão, Infraestruturas de Mercado e Pagamentos	Banco Central Europeu	Autoridade Reguladora
Killian Clifford	Diretor de Política e Advocacia	GSMA	Organismo da Indústria
Munir Bello	Líder Técnico de Certificação Mobile Money	GSMA	Organismo da Indústria
Brian Muthiora	Diretor Regulatório, Mobile Money	GSMA	Organismo da Indústria
Julieta Maina	Gerente de Advocacia e Regulamentação, Mobile Money	GSMA	Organismo da Indústria
Daniel Schwartz	Diretor, Assuntos de Política Global	Mastercard	Organismo da Indústria
Amina Tirana	Líder de Política, Pesquisa e Medição, Impacto Social	Visa	Organismo da Indústria
Miguel Nunes	Chefe de Assessoria Governamental	Visa	Organismo da Indústria
Frank Adelmann	Especialista do Setor Financeiro (Cibersegurança)	FMI	Organismo Internacional
Vijay Mauree	Coordenador do Programa, Departamento de Grupo de Estudos, TSB	ITU	Organismo de Padrões Internacionais
David Medine	Conselheiro Sénior	GCAP	Organismo Internacional
Seán Doyle	Líder de Projeto, Governança e Política de Cibersegurança	Fórum Económico Mundial	Organismo Internacional
Leon Perlman	-	Independente	Especialista no setor
David Cracknell	-	Primeiros Princípios	Especialista no setor
Abbie Barbir	-	FIDO Alliance	Especialista no setor
Dave Birch	-	Consulte o Hyperion	Especialista no setor

Alliance for Financial Inclusion
AFI, Sasana Kijang, 2, Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia
t +60 3 2776 9000 **e** info@afi-global.org www.afi-global.org

Alliance for Financial Inclusion AFI.History @NewsAFI @afinetwork